

Foreword by
Dr. Kamlesh Bajaj, Data Security Council of India



CYBER SECURITY

Understanding Cyber Crimes,
Computer Forensics and Legal Perspectives



Nina Godbole • Sunit Belapure



CYBER SECURITY

Understanding Cyber Crimes, Computer Forensics and Legal Perspectives

CYBER SECURITY

Understanding Cyber Crimes, Computer Forensics and Legal Perspectives

Nina Godbole
Sunit Belapure



CYBER SECURITY

Understanding Cyber Crimes, Computer Forensics and Legal Perspectives

Copyright © 2011 by Wiley India Pvt. Ltd., 4435-36/7, Ansari Road, Daryaganj, New Delhi-110002.

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or scanning without the written permission of the publisher.

Limits of Liability: While the publisher and the authors have used their best efforts in preparing this book, Wiley and the authors make no representation or warranties with respect to the accuracy or completeness of the contents of this book, and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. There are no warranties which extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by sales representatives or written sales materials. The accuracy and completeness of the information provided herein and the opinions stated herein are not guaranteed or warranted to produce any particular results, and the advice and strategies contained herein may not be suitable for every individual. Neither Wiley India nor the authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Disclaimer: While every effort has been made to trace copyright holders, trademark holders and obtain permission, any omissions are inadvertent and will be rectified in future editions if brought to our notice. The contents of this book have been checked for accuracy. Since deviations cannot be precluded entirely, Wiley or its authors cannot guarantee full agreement. As the book is intended for educational purpose, Wiley or its authors shall not be responsible for any errors, omissions or damages arising out of the use of the information contained in the book. This publication is designed to provide accurate and authoritative information with regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services.

Trademarks: All brand names and product names used in this book are trademarks, registered trademarks, or trade names of their respective holders. Wiley is not associated with any product or vendor mentioned in this book.

The links to URL's and video clips provided at the end of each chapter were active at the time of writing the book. The status of these being active or inactive is beyond the control of authors. For illustrations, case studies and examples, if any similarities are found between situations described and/or real individuals, then it is purely a coincidence. Due care has been taken to provide correct nomenclature of Indian IT Act and other related laws. Any subsequent changes to these are beyond the control of the authors. Mentions of products/tools/services found in this book are merely to illustrate the points made or to give examples; by no means it is an attempt to directly/indirectly/implicitly/explicitly promote those products/tools/services.

Other Wiley Editorial Offices:

John Wiley & Sons, Inc. 111 River Street, Hoboken, NJ 07030, USA

Wiley-VCH Verlag GmbH, Pappelallee 3, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 42 McDougall Street, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada, M9W 1L1

First Edition: 2011

ISBN: 978-81-265-2179-1

www.wileyindia.com

ISBN: 978-81-265-8050-7 (ebk)

A relaxed mind is essential to have a tireless body with hands to write...

*This book is dedicated to my family for their whole-hearted support to me
and their unconditional love and caring. I also dedicate this book to
my nephew Ritwik who is forever interested in knowing “how things work”!*

Nina Godbole

*I dedicate this book to my family. Without their patience, understanding, support
and most of all love, the completion of this work would not have been possible.*

Sunit Belapure

Foreword

India is the global hub of IT and business process outsourcing. With exports of USD 53 billion in software and services, and the industry projected to generate total revenues of about USD 73 billion dollars in the current year, this sector has the potential to grow to annual revenue of USD 225 billion by the year 2020. However, this is premised on a number of key enablers which have to be in position to ensure that India continues to remain a trusted global sourcing partner of choice for clients around the world. This includes development of IT and communications infrastructure, and education system that produces skilled engineers and professionals who can be readily deployed. A very important enabler is the establishment of a strong data protection culture and legal regime in the country to build confidence of clients in outsourcing their operations to India. India needs to develop and propagate global best practices for data security and privacy protection and encourage companies to implement the same. Notwithstanding the security preparedness of companies, however, cyber attacks on corporate and government infrastructure do take place and likely will continue. This is because the threat landscape is changing; new vulnerabilities in the applications and infrastructure keep getting discovered; these are exploited by criminals to commit cybercrimes.

Cyber criminals began by committing petty crimes in different parts of the world. But with the expansion of cyberspace, financial payoffs have increased, which, in turn, have led to the emergence of organized gangs spread over different cities across countries. Crime syndicates, which sometimes include terrorists, are increasingly visible. Cybercriminals have different motives, but they can command the resources to create attack vectors in order to achieve the results they want. They may commit fraud, identity theft, steal money; commit robbery against corporations, banks, nations, regions and even individuals. They steal corporate intellectual property. They also steal sensitive military and other national information in what is known as cyber espionage. With more e-governance projects being rolled out by governments at the Centre, in States and even at municipal levels, citizen services delivered over the Internet can be disrupted by cyber criminals. Their final frontier is attack on critical information infrastructures of nations which can result in outcomes similar to those achieved in traditional wars. For example, telecom networks, banking networks and energy distribution systems can be cyber attacked resulting in disruption of economy. Air traffic control systems and other infrastructures can similarly be disrupted by cyber criminals. As more and more critical infrastructures get connected to the Internet, and take advantage of increased bandwidths and new applications deployed over mobile devices, vulnerability to cyber attacks further increases. Finally, cyber crimes can be committed by nations against others in what is known as information warfare or cyber warfare. Estonia and Georgia were recently the victims of such attacks.

Cybercrimes, therefore, need to be given an effective response. We need to train not only our law enforcement agencies including police, public prosecutors, and judiciary, but also to create awareness on cyber security and cybercrimes among the people at large. This book on cybercrimes and cyber security is very timely, and I am happy to see that it deals with these topics comprehensively. It introduces the idea of cybercrimes and explains how they are planned. Vulnerability of mobile and wireless devices, which are getting exploited to commit cybercrimes, and the tools and methods used in exploiting these vulnerabilities are explained. Cyber forensics is covered in fair detail to make the reader understand the tools and the importance of their use to collect and present evidence so as to be

acceptable in a court of law. The authors, with their practical experience of dealing with cybercrimes, and in working with the corporate world to secure their systems, have brought out a very useful book that can serve both as an introductory text and a useful guide to the practitioners who may want to dive deep into specific topics.

Dr. Kamlesh Bajaj
Chief Executive Officer
Data Security Council of India
Delhi, India
December 2010

About Dr. Kamlesh Bajaj

Dr. Kamlesh Bajaj is CEO, Data Security Council of India. He has over 30 years of experience in various capacities in the IT industry. Prior to joining NASSCOM, he was the Global Head, Information Risk Management Practice, Global Consulting Practice, TCS. He was the Founder Director of Computer Emergency Response Team (CERT-In), Ministry of Communications and IT. He was the co-chair of Indo-US Cyber Security Forum for a year. As the Deputy Controller of Certifying Authorities, he established the techno-legal framework for public key infrastructure in the country. Before that, he served as a Deputy Director General, National Informatics Centre (NIC). He led large projects in Finance and Banking, most notable being the Customs EDI Project that introduced near paperless working, based on workflow, in the custom houses in India.

Dr. Bajaj established a vigorous work plan of DSCI under which best practices for data security and privacy protection; and frameworks have been developed. In his role of public advocacy, he has authored, and presented, policy papers on reasonable security practices, encryption policy, extending of binding corporate rules to the service providers under the EU Data Protection Directive, and recommendations on the proposed privacy law in the country. He has commented on the security and privacy concerns of the UID project, and presented the same at RISE international conference on security, privacy and ethics of biometrics. He has written several articles on the stronger data protection regime under the IT (Amendment) Act, 2008; and delivered talks on cyber crimes and cyber security; and privacy protection. He has established the footprint of DSCI as a key organization engaged in data protection through increased visibility in national and international conferences. He is engaged in building DSCI into a self-regulatory organization using best practices, acceptance by regulators in other countries, speedier trial of cyber crimes, and dispute resolution by developing an ecosystem around DSCI.

About DSCI (Data Security Council of India) and NASSCOM

NASSCOM® is the premier trade body and the chamber of commerce of the IT-BPO industries in India. NASSCOM is a global trade body with more than 1200 members, which include both Indian and multi-national companies that have a presence in India.

Data Security Council of India (DSCI), a section 25 not-for-profit company, was setup as an independent Self Regulatory Organization (SRO) by NASSCOM, to promote data protection, develop security and privacy codes & standards and encourage the IT/BPO industry to implement the same. DSCI has developed Best Practices for Data Protection that are in line with global standards and cover emerging disciplines of security and privacy. While its immediate goal is to raise the level of security and privacy of IT and BPO service providers to assure their clients and other stakeholders that India is a secure destination for global sourcing, DSCI also promotes these best practices for domestic industry segments like Banking, Telecom and E-governance.

About the Authors

Nina Godbole is an author of the book *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* published by Wiley India in January 2009. She has published numerous articles on topics in leading IT magazines. She is also on the Editorial Board of IEEE Computer Society for their IT Professional bimonthly publication. Her current domain of work is business controls and regulatory compliance with focus on data privacy and information security.

The author has a vast experience in the IT industry in Software Quality Assurance, system analysis and design, business development and support services, training, quality management, operations management, design and implementation of computer-based MIS applications. The author was instrumental in preparing IT perspective plans for the client organizations as well as BPR initiatives, analysis for ERP package deployment patterns in the USA and as a systems analyst for Web-based application in France. She has played an instrumental role in several successfully driven organizational initiatives – the ISO, P-CMM, and CMM-I.



The author is an active member of professional bodies and academic research groups: ISACA-USA, PMI-USA, the Mobile Internet Research and Applications Group (MIRAG) at an Australian University, SW Process Improvement Network (SPIN), Institute of Management Consultants of India (IMCI), Computer Society of India (CSI) and Pune Management Association (PMA).

Nina Godbole holds a Masters degree from IIT, Bombay and MS Engineering (Computer Science) degree from Newport University, USA. She has several international professional certifications to her credit – CIPP/IT from IAPP (International Association of Privacy Professionals, USA) CQA, CSTE from the QAI-USA, CISA from ISACA-USA, BVQI Certified ISO Auditor and a certified PMP from PMI.

The author is also an ITIL foundation certified professional and has handled numerous training workshops and seminars in her domain of expertise. She is a key speaker at many conferences and visiting faculty to many institutes including those under Pune University as well as CDAC in the past. She has also addressed overseas students at Australian universities as the guest faculty. As a CISA, she is actively involved in security audit engagements for business units of the organization in India as well as for overseas customer accounts.

Sunit Belapure has more than 8 years experience in Information Security domain out of his total industry experience of more than 18 years. He works in the domain of ISRM (Information Security and Risk and Management) and Information System Audit. Sunit has respective international certifications to his credit – CISA (Certified Information Systems Auditor) from ISACA-USA, IRCA certified ISO 27001:2005 Lead Auditor, Certified Ethical Hacker (CEH v5.0) from EC-Council-USA and CISM (Certified Information Security Manager) from ISACA-USA. He is a member of ISACA, USA. He engages into Compliance and Assurance assignments (for ERP as well as for



Non-ERP applications) under IS security and IT Governance domain. He was instrumental in building an Internal Audit Team for IT Compliance Audits as a part of his on-site assignment for 3.1/2 years in USA into a global automobile organization. Sunit is a noted speaker on Information Security domain at reputed institutes in and around Pune.

Preface

Why this Book?

A “Globalization” phenomenon has been one of the remarkable developments in the last few decades. IT (Information Technology) has made unbelievable strides. Today we witness its convergence with Communication Technology, that is, ICT (Information and Communication Technology). This book is about understanding risks in cyber space where we use IT, ICT and the Internet for many reasons. We are “netizens,” considering the amount of time we spend on the Internet and our dependence on the Internet. The range of technology users (ICT, mobile technology and Internet subscribers) is wide – school children to teenagers, adults, business professionals and now even senior citizens who use the Net while chatting with their children overseas. We are in a 24×7 interconnected world where data and information changes hands at a frequency and speed like never before. We must understand the perils as well as advantages of the technology. We should be smart users – we should reap the benefits of the modern computer and communication technology and yet should steer clear of trouble. This book was envisaged and is delivered with these thoughts in mind. It is an awareness creation book plus more than just that.

Cyber Security is a Critical Area

As per a survey of 2009, in which 500 small and mid-sized business (SMB) companies were contacted, it was found that almost half of those companies considered cyber crime as the threat only for larger organizations. Although SMB organizations are generally aware of the challenges and threats in the cyber space, typically, they do not have the dedicated time or resources to completely protect themselves. SMBs do not take cyber threats seriously enough – until after they get hit! Our exponentially growing dependence on IT is a fact. Today we talk of “information warfare” and it can hit a nation. The ramifications of cyber threats are beyond just individuals and organizations.

Imagine this – new wars will be fought in a completely different fashion. Perhaps there would be no need to send a battalion of soldiers covered by air attacks. It could just be sufficient to completely breakdown critical IT infrastructure of a nation. May be the enemy could launch simultaneous DoS attacks or Distributed DoS attacks on critical servers of a nation such as the telecom company servers, ISP servers, etc. We are in a mobile computing era supported by wireless networks and mobile work force. The victims and the attackers need not be physically juxtaposed.

“Netizens” must be wary of the “double-edged” power of information technology in the cyber space. Like any other technology, IT can be put to both good and bad use. Mobile phones and laptops are common items, in fact, objects of necessity in the modern urban area. Given the fact that ICT is now the media of disseminating knowledge and information, the penetration rate of computers, laptops, mobile phones and to some extent even wireless networks is only going to increase in the coming years. In this milieu we must be aware of cyber threats to which we all are potential targets. Understanding of cyber attacks such as Phishing and Identity Theft are important because they are on the rise and we encounter them in our day-to-day life. We must know enough to avoid being victims of perpetrators.

Motivation for this Book

Attention to “Cyber Security” is the need of the hour for the reasons mentioned. Lead Author’s, Nina Godbole’s, previous book on the topic of Information Systems Security titled (*Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*) has been a great success. Our primary motivation came from the thought for delivering an equally good book on the topic of cyber security. There is a strong link between this book and *Information Systems Security*. Although the two books go well together and serve as valuable knowledge assets, however, this book can also be used as a stand-alone book on its own. Cyber security is an emerging topic – SMBs need to take cyber security seriously. Considering this is another aspect of what motivated us to take up this project. Educational institutes looking for a good book on cyber security topic will be more than happy to have this book.

Audience for this Book

Anyone who is curious about cyber space, threats, crimes and investigation therein should read this book. This book creates awareness through simple practical tips and tricks, and educates readers to learn how to avoid becoming victims of cyber crimes. Thus, the book is meant for a wide range of audience – students, individual readers, corporate management professionals, law students, police officers and other law enforcement agencies. Small and medium enterprises indeed need to focus on some of the key threat vectors. They need to protect the endpoint (servers and workstations and even hand-held devices used by employees for business work) from malware and other threats. They need to protect their users from dangers on the Web – this is the fastest growing new source of infection. They need to protect their users from Spam – between 85% and 95% of the world’s E-Mail is spammed and 25% of that contains some Malicious Code or pushes users to a malicious website. They need to protect their data – both at rest and in transit. Confidential data gets lost by either accident or through malicious acts. Prevention is required and we make our readers aware about this.

This book is designed with a broad audience in mind – individuals, who wish to take up cyber forensics as career as well as those who want to seek careers in cyber security and managers from organization who want to take cyber security seriously should also read this book. Keeping this intended audience in mind, the book is packed with adequate technical details as well as material with value to management.

Structure of this Book

The book consists a total of 12 Chapters. The book includes Chapters 1–9 and the companion CD includes remaining 3 Chapters (Chapters 10–12) as indicated in the Table of Contents. Chapter 11 has all the examples, illustrative scenarios from real-life incidents to amplify the concepts addressed from Chapters 1 to 10. Chapter 12 provides valuable advice on cyber security career and related certifications.

For readers’ convenience, the organization of all the examples and illustrations in Chapter 11 is presented with chapter structure information in the Introduction section and in detail with the table of contents in each subsection of Chapter 11.

Although you may not want to read the book in a sequential order, we strongly recommend that you start with Chapter 1 to get a good overview of the cyber security and cyber crime arena. Then onward you can proceed to pick up a topic of your interest from Chapters 2 to 10. You can also take up Chapter 11

after reading Chapter 1. For almost all examples and illustrations inside Chapter 11, we have provided linkages to chapters that address the underlying concepts.

At the end of each chapter the related appendices are mentioned – they serve as extended material to that chapter. While we have mentioned at the end of each chapter, only the alphabetical number of the related appendices, however, in the Table of Contents, you can see the name of topic(s) handled in the appendices. For each chapter, extended material that is useful in the context of the chapter is provided under *REFERENCES*. In addition, we have pointed out some useful material for each chapter; at the end of chapter, you will find additional sections called *FURTHER READING* – there are two subsections under that: *Additional Useful Web References, Books, Articles and Research Papers* and *Video Clips*. You should benefit from the additional material listed in these sections.

Appendices, Case Illustrations and the CD Companion of this Book

The appendices are in the CD companion of the book. Appendices carry valuable material that serves as extension to most chapters. Therefore, it is important to note related appendices mentioned at the end of each chapter. The guidelines, checklists, useful forms and templates in the appendices are resourceful. Do use them to your full benefit. Appendices O–T pertain to related laws that are important in the context of cyber security and cyber crime (The Indian IT Act, Indian Penal Code, Indian Evidence Act, Indian Patent Act, Indian Trademark Act and Indian Copyright Act). Data Security Framework and Data Privacy Framework addressed in Appendix U and Appendix V, respectively, are very important – the pioneering work of Data Security Council of India (DSCI) is introduced in these chapters.

Semantics and Nomenclature

We have made the best attempt to maintain gender neutrality in the book with use of the term he/she. When an acronym occurs for the first time, it is mentioned with a full form; thereafter, however, only the acronym is used. Should the occurrence of the acronym be repeating after a long time, and if space permits, we have again mentioned the full form. In some place, we may not have presented the full form only due to want of space; our apologies for that. The important points to be noted are highlighted with an icon (pencil in a hand). Regarding “Amendment to Indian IT Act 2008,” we have used the term ITA 2008 to denote this throughout the book. You should noted that in other works, you may also come across the term ITAA 2008 denoting the same, that is, IT (Amended) Act 2008.

Authors' Message from this Book

New technologies such as the Internet have drastically changed our methods of communication, way of conducting business and even the ways we use for engaging in recreation. The Internet provides us both speed and convenience to attract a critical mass of global users. We should be aware that Internet transgressors also adopt the medium as a new avenue for crime. While larger organizations have the wherewithal to fight cyber threats, the ability to fight cyber attacks should exist with SMBs. Knowing fully well that, larger organizations are better off with security infrastructure, cyber criminals consider SMBs as their easier target. These small and medium organizations are operating in an increasingly competitive environment and tough economic climate. They are becoming more and more reliant on the Internet (e.g., cloud computing) to grow and succeed but are in denial about cyber security threats. Irrespective of the size of business, viruses, hacker intrusions, Spyware and Spam can lead to lost or stolen data,

computer downtime, decreased productivity, compliance issues, lost sales and even loss of reputation. Just because a business is small, it does not mean it is immune to security threats. Cyber criminals operate as a global gang and they do not care of organizational and national boundaries.

Nina Godbole
Sunit Belapure
March 2011

Acknowledgments

First and foremost, I thank Wiley India for the opportunity to complete yet another project. This time it was an even more onerous task, given the success of my previous comprehensive book on *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* published by Wiley India Pvt. Ltd., January 2009. Special thanks to Vikas Gupta (MD) and Paras Bansal (Publisher), Wiley India Pvt. Ltd, for their extraordinary support.

I am indebted to Dr. Kamlesh Bajaj, CEO, Data Security Council of India (DSCI) for blessing this book with the wonderful foreword. I am also thankful to Vinayak Godse, Director – Data Protection, DSCI for the permission to introduce DSCI's frameworks for Data Privacy and Data Security.

I owe very special thanks to Advocate Vaishali Bhagwat for the valuable guidance she provided on the legal aspects. Without her feedback I would not have been able to complete the chapters containing legal side of cyber crime and cyber security. My discussions with her truly helped me clarify many ideas. My dear friend Sandeep Godbole was instrumental in reviewing some of the chapters and I thank him for that special help.

While I developed the major part of this work, Co-Author Sunit did his small bit of contribution as well. He had approached me with a good thought for developing a book to build awareness about cyber crime. I thought the best way to approach such a work would be to address cyber crimes in the context of "cyber security" which is much a larger domain. I recognize Sunit's contribution to this project as well as his enthusiasm with sustained effort throughout this project.

We are fortunate to have a very competent team from Wiley India supporting us on this book project. My sincere thanks to the Editorial team lead by Meenakshi Sehrawat (Senior Developmental Editor) and her colleague Rakhee Das for their valuable support during the editorial phase. I also thank the other key contributing teams at Wiley India – creative team for the cover and design, the entire production team for preparing/packaging of this book and the marketing team lead by Abhishek Bhardwaj.

There are institutes and individuals who graciously allowed us to use various statistics and diagrams that were essential to add as part of explanations and/or to emphasize key points in each chapter. We are thankful to Dr. Simon Bramble, Head of Police Science and Forensics at the National Policing Improvement Agency (NPIA), Confederation of Indian Industries (CII), Aparajita Sikdar and Jaspreet Kaur from the ICICI Bank, Sebastian Edassery, Brian Carrier, Sagar Desai of Symantec, Supriya Kulkarni. Thanks also to my source of inspirations and distant role models in security/privacy domain – Dr. Lorrie Faith Cranor, Privacy Research Lab at the Carnegie Mellon University, who was also the instructor during the special Information Privacy Certification I completed during this project; Dr. Larry Ponemon, Ponemon Institute; Harriet Pearson, IBM; Australian Privacy Expert, Roger Clarke.

In addition, I wish to thank the following individuals who helped in one way or the other - listening to my ideas for this book, adding their thoughts, giving us time during our research and verification questions, giving me the opportunity to run workshops related to cyber security which greatly helped during the development of this book, keeping the laptop up and running to ensure uptime for scripting the work, keeping the author in physical fitness and so many other things. If some names got missed out then that could be only due to an oversight and not by intention:

Dr. Sanjay Tungar
Neelima Gaikwad

Vicky Shah
Vikram Wadgama

Harshada Bapat
S.D. Puranik

Nina Godbole
March 2011

I thank the Lead Author, Nina Godbole, for providing me the opportunity to work with her on this project. The great success of her previous comprehensive book on “Information System Security” laid down a solid foundation for this project. I learnt so much from her in the course of this project and I am grateful to her for mentoring me on the skills of writing which is so important for me as the first time author.

My sincere thanks to Wiley India team for their support and co-operation on this project – special thanks to the Editorial team lead by Meenakshi Sehrawat and her colleague Rakhee Das.

Sunit Belapure
March 2011

Contents

Foreword	vii
About Dr. Kamlesh Bajaj	ix
About the Authors	xi
Preface	xiii
Acknowledgments	xvii
List of Figures	xxxiii
List of Tables	xxxix
List of Boxes	xliii

1	Introduction to Cybercrime	1
	Learning Objectives	1
1.1	Introduction	1
1.2	Cybercrime: Definition and Origins of the Word	1
1.3	Cybercrime and Information Security	13
1.4	Who are Cybercriminals?	16
1.5	Classifications of Cybercrimes	17
	1.5.1 <i>E-Mail Spoofing</i>	18
	1.5.2 <i>Spamming</i>	18
	1.5.3 <i>Cyberdefamation</i>	19
	1.5.4 <i>Internet Time Theft</i>	21
	1.5.5 <i>Salami Attack/Salami Technique</i>	21
	1.5.6 <i>Data Diddling</i>	21
	1.5.7 <i>Forgery</i>	22
	1.5.8 <i>Web Jacking</i>	22
	1.5.9 <i>Newsgroup Spam/Crimes Emanating from Usenet Newsgroup</i>	22
	1.5.10 <i>Industrial Spying/Industrial Espionage</i>	22
	1.5.11 <i>Hacking</i>	23
	1.5.12 <i>Online Frauds</i>	23
	1.5.13 <i>Pornographic Offenses</i>	27
	1.5.14 <i>Software Piracy</i>	28
	1.5.15 <i>Computer Sabotage</i>	28
	1.5.16 <i>E-Mail Bombing/Mail Bombs</i>	30
	1.5.17 <i>Usenet Newsgroup as the Source of Cybercrimes</i>	30
	1.5.18 <i>Computer Network Intrusions</i>	30
	1.5.19 <i>Password Sniffing</i>	30
	1.5.20 <i>Credit Card Frauds</i>	31
	1.5.21 <i>Identity Theft</i>	31
1.6	Cybercrime: The Legal Perspectives	32
1.7	Cybercrimes: An Indian Perspective	32

1.8	Cybercrime and the Indian ITA 2000	34
	<i>1.8.1 Hacking and the Indian Law(s)</i>	34
1.9	A Global Perspective on Cybercrimes	36
	<i>1.9.1 Cybercrime and the Extended Enterprise</i>	38
1.10	Cybercrime Era: Survival Mantra for the Netizens	39
1.11	Concluding Remarks and Way Forward to Further Chapters	39
	Summary	40
	Review Questions	40
	References	40
	Further Reading	42
2	Cyberoffenses: How Criminals Plan Them	45
	Learning Objectives	45
2.1	Introduction	45
	<i>2.1.1 Categories of Cybercrime</i>	48
2.2	How Criminals Plan the Attacks	49
	<i>2.2.1 Reconnaissance</i>	50
	<i>2.2.2 Passive Attacks</i>	50
	<i>2.2.3 Active Attacks</i>	54
	<i>2.2.4 Scanning and Scrutinizing Gathered Information</i>	58
	<i>2.2.5 Attack (Gaining and Maintaining the System Access)</i>	61
2.3	Social Engineering	61
	<i>2.3.1 Classification of Social Engineering</i>	62
2.4	Cyberstalking	65
	<i>2.4.1 Types of Stalkers</i>	66
	<i>2.4.2 Cases Reported on Cyberstalking</i>	66
	<i>2.4.3 How Stalking Works?</i>	66
	<i>2.4.4 Real-Life Incident of Cyberstalking</i>	67
2.5	Cybercafe and Cybercrimes	67
2.6	Botnets: The Fuel for Cybercrime	71
	<i>2.6.1 Botnet</i>	71
2.7	Attack Vector	73
2.8	Cloud Computing	75
	<i>2.8.1 Why Cloud Computing?</i>	76
	<i>2.8.2 Types of Services</i>	77
	<i>2.8.3 Cybercrime and Cloud Computing</i>	77
	Summary	79
	Review Questions	79
	References	79
	Further Reading	80
3	Cybercrime: Mobile and Wireless Devices	81
	Learning Objectives	81
3.1	Introduction	81
3.2	Proliferation of Mobile and Wireless Devices	82

3.3	Trends in Mobility	84
3.4	Credit Card Frauds in Mobile and Wireless Computing Era	87
	3.4.1 <i>Types and Techniques of Credit Card Frauds</i>	88
3.5	Security Challenges Posed by Mobile Devices	91
3.6	Registry Settings for Mobile Devices	92
3.7	Authentication Service Security	93
	3.7.1 <i>Cryptographic Security for Mobile Devices</i>	93
	3.7.2 <i>LDAP Security for Hand-Held Mobile Computing Devices</i>	94
	3.7.3 <i>RAS Security for Mobile Devices</i>	95
	3.7.4 <i>Media Player Control Security</i>	98
	3.7.5 <i>Networking API Security for Mobile Computing Applications</i>	98
3.8	Attacks on Mobile/Cell Phones	99
	3.8.1 <i>Mobile Phone Theft</i>	99
	3.8.2 <i>Mobile Viruses</i>	101
	3.8.3 <i>Mishing</i>	101
	3.8.4 <i>Vishing</i>	102
	3.8.5 <i>Smishing</i>	103
	3.8.6 <i>Hacking Bluetooth</i>	105
3.9	Mobile Devices: Security Implications for Organizations	107
	3.9.1 <i>Managing Diversity and Proliferation of Hand-Held Devices</i>	107
	3.9.2 <i>Unconventional/Stealth Storage Devices</i>	108
	3.9.3 <i>Threats through Lost and Stolen Devices</i>	110
	3.9.4 <i>Protecting Data on Lost Devices</i>	111
	3.9.5 <i>Educating the Laptop Users</i>	111
3.10	Organizational Measures for Handling Mobile Devices-Related Security Issues	112
	3.10.1 <i>Encrypting Organizational Databases</i>	113
	3.10.2 <i>Including Mobile Devices in Security Strategy</i>	113
3.11	Organizational Security Policies and Measures in Mobile Computing Era	114
	3.11.1 <i>Importance of Security Policies relating to Mobile Computing Devices</i>	114
	3.11.2 <i>Operating Guidelines for Implementing Mobile Device Security Policies</i>	115
	3.11.3 <i>Organizational Policies for the Use of Mobile Hand-Held Devices</i>	116
3.12	Laptops	116
	3.12.1 <i>Physical Security Countermeasures</i>	117
	Summary	120
	Review Questions	121
	References	121
	Further Reading	122
4	Tools and Methods Used in Cybercrime	125
	Learning Objectives	125
4.1	Introduction	125
4.2	Proxy Servers and Anonymizers	129

4.3	Phishing	131
	4.3.1 <i>How Phishing Works?</i>	131
4.4	Password Cracking	132
	4.4.1 <i>Online Attacks</i>	134
	4.4.2 <i>Offline Attacks</i>	134
	4.4.3 <i>Strong, Weak and Random Passwords</i>	135
	4.4.4 <i>Random Passwords</i>	136
4.5	Keyloggers and Spywares	137
	4.5.1 <i>Software Keyloggers</i>	137
	4.5.2 <i>Hardware Keyloggers</i>	140
	4.5.3 <i>Antikeylogger</i>	140
	4.5.4 <i>Spywares</i>	140
4.6	Virus and Worms	143
	4.6.1 <i>Types of Viruses</i>	146
4.7	Trojan Horses and Backdoors	151
	4.7.1 <i>Backdoor</i>	152
	4.7.2 <i>How to Protect from Trojan Horses and Backdoors</i>	153
4.8	Steganography	155
	4.8.1 <i>Steganalysis</i>	158
4.9	DoS and DDoS Attacks	158
	4.9.1 <i>DoS Attacks</i>	158
	4.9.2 <i>Classification of DoS Attacks</i>	159
	4.9.3 <i>Types or Levels of DoS Attacks</i>	160
	4.9.4 <i>Tools Used to Launch DoS Attack</i>	161
	4.9.5 <i>DDoS Attacks</i>	162
	4.9.6 <i>How to Protect from DoS/DDoS Attacks</i>	163
4.10	SQL Injection	164
	4.10.1 <i>Steps for SQL Injection Attack</i>	165
	4.10.2 <i>How to Prevent SQL Injection Attacks</i>	167
4.11	Buffer Overflow	168
	4.11.1 <i>Types of Buffer Overflow</i>	168
	4.11.2 <i>How to Minimize Buffer Overflow</i>	170
4.12	Attacks on Wireless Networks	171
	4.12.1 <i>Traditional Techniques of Attacks on Wireless Networks</i>	176
	4.12.2 <i>Theft of Internet Hours and Wi-Fi-based Frauds and Misuses</i>	177
	4.12.3 <i>How to Secure the Wireless Networks</i>	179
	Summary	180
	Review Questions	181
	References	181
	Further Reading	183
5	Phishing and Identity Theft	185
	Learning Objectives	185
5.1	Introduction	185

5.2	Phishing	187
	<i>5.2.1 Methods of Phishing</i>	191
	<i>5.2.2 Phishing Techniques</i>	193
	<i>5.2.3 Spear Phishing</i>	195
	<i>5.2.4 Types of Phishing Scams</i>	196
	<i>5.2.5 Phishing Toolkits and Spy Phishing</i>	201
	<i>5.2.6 Phishing Countermeasures</i>	202
5.3	Identity Theft (ID Theft)	206
	<i>5.3.1 Personally Identifiable Information(PII)</i>	209
	<i>5.3.2 Types of Identity Theft</i>	211
	<i>5.3.3 Techniques of ID Theft</i>	218
	<i>5.3.4 Identity Theft: Countermeasures</i>	220
	<i>5.3.5 How to Efface Your Online Identity</i>	220
	Summary	221
	Review Questions	222
	References	222
	Further Reading	224
6	Cybercrimes and Cybersecurity: The Legal Perspectives	227
	Learning Objectives	227
6.1	Introduction	227
6.2	Cybercrime and the Legal Landscape around the World	230
	<i>6.2.1 A Broad View on Cybercrime Law Scenario in the Asia-Pacific Region</i>	231
	<i>6.2.2 Online Safety and Cybercrime Laws: Detailed Perspective on the Current Asia-Pacific Scenario</i>	233
	<i>6.2.3 Anti-Spam Laws in Canada</i>	243
	<i>6.2.4 Cybercrime and Federal Laws in the US</i>	245
	<i>6.2.5 The EU Legal Framework for Information Privacy to Prevent Cybercrime</i>	247
	<i>6.2.6 Cybercrime Legislation in the African Region</i>	249
6.3	Why Do We Need Cyberlaws: The Indian Context	253
6.4	The Indian IT Act	254
	<i>6.4.1 Admissibility of Electronic Records: Amendments made in the Indian ITA 2000</i>	264
	<i>6.4.2 Positive Aspects of the ITA 2000</i>	269
	<i>6.4.3 Weak Areas of the ITA 2000</i>	270
6.5	Challenges to Indian Law and Cybercrime Scenario in India	271
6.6	Consequences of Not Addressing the Weakness in Information Technology Act	272
6.7	Digital Signatures and the Indian IT Act	273
	<i>6.7.1 Public-Key Certificate</i>	273
	<i>6.7.2 Representation of Digital Signatures in the ITA 2000</i>	274
	<i>6.7.3 Impact of Oversight in ITA 2000 Regarding Digital Signatures</i>	275
	<i>6.7.4 Implications for Certifying Authorities</i>	277

	6.7.5 <i>The Current Scenario Regarding Digital Signatures under the Indian IT Act</i>	278
	6.7.6 <i>Cryptographic Perspective on the Indian IT Act</i>	279
6.8	Amendments to the Indian IT Act	282
	6.8.1 <i>Overview of Changes Made to the Indian IT Act</i>	283
	6.8.2 <i>Cybercafe-Related Matters Addressed in the Amendment to the Indian IT Act</i>	289
	6.8.3 <i>State Government Powers Impacted by the Amendments to the Indian IT Act</i>	293
	6.8.4 <i>Impact of IT Act Amendments on Information Technology Organizations</i>	295
6.9	Cybercrime and Punishment	305
6.10	Cyberlaw, Technology and Students: Indian Scenario	307
	Summary	309
	Review Questions	310
	References	311
	Further Reading	312
7	Understanding Computer Forensics	317
	Learning Objectives	317
7.1	Introduction	317
7.2	Historical Background of Cyberforensics	318
7.3	Digital Forensics Science	320
7.4	The Need for Computer Forensics	323
7.5	Cyberforensics and Digital Evidence	327
	7.5.1 <i>The Rules of Evidence</i>	329
7.6	Forensics Analysis of E-Mail	332
	7.6.1 <i>RFC2822</i>	338
7.7	Digital Forensics Life Cycle	339
	7.7.1 <i>The Digital Forensics Process</i>	339
	7.7.2 <i>The Phases in Computer Forensics/Digital Forensics</i>	341
	7.7.3 <i>Precautions to be Taken when Collecting Electronic Evidence</i>	353
7.8	Chain of Custody Concept	355
7.9	Network Forensics	357
7.10	Approaching a Computer Forensics Investigation	358
	7.10.1 <i>Typical Elements Addressed in a Forensics Investigation Engagement Contract</i>	359
	7.10.2 <i>Solving a Computer Forensics Case</i>	361
7.11	Setting up a Computer Forensics Laboratory: Understanding the Requirements	362
7.12	Computer Forensics and Steganography	368
	7.12.1 <i>Rootkits</i>	370
	7.12.2 <i>Information Hiding</i>	371
7.13	Relevance of the OSI 7 Layer Model to Computer Forensics	373
	7.13.1 <i>Step 1: Foot Printing</i>	373

7.13.2	<i>Step 2: Scanning and Probing</i>	375
7.13.3	<i>Step 3: Gaining Access</i>	376
7.13.4	<i>Step 4: Privilege</i>	376
7.13.5	<i>Step 5: Exploit</i>	376
7.13.6	<i>Step 6: Retracting</i>	376
7.13.7	<i>Step 7: Installing Backdoors</i>	376
7.14	Forensics and Social Networking Sites: The Security/Privacy Threats	377
7.15	Computer Forensics from Compliance Perspective	383
	<i>7.15.1 The Regulatory Perspective for Forensics at the International Level</i>	384
	<i>7.15.2 Computer Forensics Compliance Requirements: Implications for Evidential Aspects</i>	388
	<i>7.15.3 Computer Forensics Expertise Status in India</i>	389
7.16	Challenges in Computer Forensics	389
	<i>7.16.1 Technical Challenges: Understanding the Raw Data and its Structure</i>	390
	<i>7.16.2 The Legal Challenges in Computer Forensics and Data Privacy Issues</i>	392
7.17	Special Tools and Techniques	396
	<i>7.17.1 Digital Forensics Tools Ready Reckenor</i>	397
	<i>7.17.2 Special Technique: Data Mining used in Cyberforensics</i>	402
7.18	Forensics Auditing	403
7.19	Antiforensics	406
	Summary	408
	Review Questions	409
	References	410
	Further Reading	415
8	Forensics of Hand-Held Devices	423
	Learning Objectives	423
8.1	Introduction	423
8.2	Understanding Cell Phone Working Characteristics	425
	<i>8.2.1 Understanding the Types of Cellular Networks</i>	426
	<i>8.2.2 NTT DoCoMo</i>	428
	<i>8.2.3 Cell Phones: Hardware and Software Features</i>	430
8.3	Hand-Held Devices and Digital Forensics	431
	<i>8.3.1 Mobile Phone Forensics</i>	433
	<i>8.3.2 PDA Forensics</i>	438
	<i>8.3.3 Printer Forensics</i>	440
	<i>8.3.4 Scanner Forensics</i>	442
	<i>8.3.5 Smartphone Forensics</i>	442
	<i>8.3.6 iPhone Forensics</i>	445
	<i>8.3.7 Challenges in Forensics of the Digital Images and Still Camera</i>	454
	<i>8.3.8 Forensics of the BlackBerry Wireless Device</i>	458
8.4	Toolkits for Hand-Held Device Forensics	463
	<i>8.4.1 EnCase</i>	464

8.4.2	<i>Device Seizure and PDA Seizure</i>	464
8.4.3	<i>Palm DD (PDD)</i>	465
8.4.4	<i>Forensics Card Reader</i>	466
8.4.5	<i>Cell Seizure</i>	466
8.4.6	<i>MOBILedit!</i>	466
8.4.7	<i>ForensicSIM</i>	467
8.5	Forensics of iPods and Digital Music Devices	467
8.5.1	<i>The New Avatar of Digital Music Hand-Held Devices</i>	467
8.5.2	<i>Understanding iPod Features and iPod Forensics Techniques</i>	469
8.5.3	<i>iPod Forensics: Evidence Handling and Crime Scene Considerations</i>	472
8.6	An Illustration on Real Life Use of Forensics	474
8.7	Techno-Legal Challenges with Evidence from Hand-Held Devices	475
8.7.1	<i>Role of Computer Forensics in Litigations</i>	476
8.7.2	<i>Challenges Due to Forensics Validity Issues about Evidences</i>	479
8.7.3	<i>Challenges to Law Enforcement Authorities</i>	479
8.7.4	<i>Toolkit Constraints</i>	480
8.7.5	<i>Generally Accepted Evidence Principles and the Difference with Hand-Held Devices</i>	481
8.7.6	<i>Mobile Phone Evidence Guidelines</i>	482
8.7.7	<i>Battery and Memory Storage Considerations from Forensics Perspective</i>	484
8.8	Organizational Guidelines on Cell Phone Forensics	484
8.8.1	<i>Hand-Held Forensics as the Specialty Domain in Crime Context</i>	484
	Summary	488
	Review Questions	488
	References	489
	Further Reading	490
9	Cybersecurity: Organizational Implications	495
	Learning Objectives	495
9.1	Introduction	495
9.1.1	<i>Insider Attack Example 1: Heartland Payment System Fraud</i>	498
9.1.2	<i>Insider Attack Example 2: Blue Shield Blue Cross (BCBS)</i>	498
9.2	Cost of Cybercrimes and IPR Issues: Lessons for Organizations	501
9.2.1	<i>Organizations have Internal Costs Associated with Cybersecurity Incidents</i>	502
9.2.2	<i>Organizational Implications of Software Piracy</i>	504
9.3	Web Threats for Organizations: The Evils and Perils	505
9.3.1	<i>Overview of Web Threats to Organizations</i>	505
9.4	Security and Privacy Implications from Cloud Computing	515
9.5	Social Media Marketing: Security Risks and Perils for Organizations	516
9.5.1	<i>Understanding Social Media Marketing</i>	517
9.5.2	<i>Best Practices with Use of Social Marketing Tools</i>	518
9.6	Social Computing and the Associated Challenges for Organizations	522

9.7	Protecting People's Privacy in the Organization	523
9.8	Organizational Guidelines for Internet Usage, Safe Computing Guidelines and Computer Usage Policy	524
	<i>9.8.1 Developing an Organizational Policy for Computer Usage</i>	526
9.9	Incident Handling: An Essential Component of Cybersecurity	531
	<i>9.9.1 Definitions and Entities Involved</i>	531
	<i>9.9.2 Why should Organizations have Incident Response Systems?</i>	537
	<i>9.9.3 Examples of Cybersecurity Incidents and the ITIL Perspective</i>	538
	<i>9.9.4 What Organizations Can Do To Protect their Systems from Cybersecurity Incidents?</i>	540
	<i>9.9.5 Best Practices for Organizations</i>	541
	<i>9.9.6 Incident Response Team Work, Capabilities and Structure</i>	544
	<i>9.9.7 Benefits from Incident Response Systems</i>	546
	<i>9.9.8 Checklists</i>	548
9.10	Forensics Best Practices for Organizations	548
	<i>9.10.1 Organizations must Understand Digital Forensics Investigation and Digital Evidences</i>	550
	<i>9.10.2 Concerns with Being a Forensically Ready Organization</i>	551
	<i>9.10.3 Key Activities for Organizations Getting Forensically Ready</i>	551
	<i>9.10.4 Benefits of Being a Forensically Ready Organization</i>	553
9.11	Media and Asset Protection: Best Practices for Organizations	554
9.12	Importance of Endpoint Security in Organizations	559
	Summary	565
	Review Questions	565
	References	566
	Further Reading	567



10 Cybercrime and Cyberterrorism: Social, Political, Ethical and Psychological Dimensions 571

	Learning Objectives	571
10.1	Introduction	571
10.2	Intellectual Property in the Cyberspace	573
	<i>10.2.1 Copyright</i>	574
	<i>10.2.2 Patent</i>	576
	<i>10.2.3 Trademarks</i>	577
	<i>10.2.4 Trade Secret</i>	578
	<i>10.2.5 Trade Name</i>	578
	<i>10.2.6 Domain Name</i>	579
10.3	The Ethical Dimension of Cybercrimes	580
	<i>10.3.1 Ethical Hackers: Good Guys in Bad Land</i>	581
10.4	The Psychology, Mindset and Skills of Hackers and Other Cybercriminals	585
	<i>10.4.1 Inside the Minds and Shoes of Hackers and Cybercriminals</i>	586
	<i>10.4.2 Hackers and Cybercriminals: Evolution of Technical Prowess and Skills</i>	587
	<i>10.4.3 Ethical Hackers</i>	590

10.5	Sociology of Cybercriminals	592
	10.5.1 <i>Personality Traits of Cybercriminals and Young Generation's Views about Hacking</i>	592
10.6	Information Warfare: Perception or An Eminent Reality?	593
	10.6.1 <i>Cyberwar Ground is HOT</i>	594
	10.6.2 <i>Cyber Jihadist on the Rise</i>	595
	Summary	597
	Review Questions	598
	References	599
	Further Reading	600
 11	Cybercrime: Illustrations, Examples and Mini-Cases	603
11.1	Learning Objectives	603
11.1	Introduction	603
11.2	Real-Life Examples	604
	11.2.1 <i>Example 1: Official Website of Maharashtra Government Hacked</i>	606
	11.2.2 <i>Example 2: E-Mail Spoofing Instances</i>	607
	11.2.3 <i>Example 3: E-Mail Bombing Involving a Foreigner</i>	608
	11.2.4 <i>Example 4: I Love You Melissa – Come Meet Me on the Internet</i>	608
	11.2.5 <i>Example 5: The "Piranhas" Tragedy with Children</i>	608
	11.2.6 <i>Example 6: Doodle me Diddle!</i>	609
	11.2.7 <i>Example 7: Ring-Ring Telephone Ring – Chatting Sessions Turn Dangerous</i>	609
	11.2.8 <i>Example 8: Young Lady's Privacy Impacted</i>	609
	11.2.9 <i>Example 9: Job Racket Exposed by Mumbai City Cybercrime Cell</i>	610
	11.2.10 <i>Example 10: Indian Banks Lose Millions of Rupees</i>	610
	11.2.11 <i>Example 11: Infinity E-Search BPO Case</i>	611
	11.2.12 <i>Example 12: Charged for Computer Intrusion</i>	612
	11.2.13 <i>Example 13: Small "Shavings" for Big Gains!</i>	612
	11.2.14 <i>Example 14: Man Goes Behind Bars for Computer Fraud Offense</i>	613
	11.2.15 <i>Example 15: "Justice" vs. "Justice" – Software Developer Arrested for Launching Website Attacks</i>	613
	11.2.16 <i>Example 16: CAN-SPAM Act Violation through E-Mail Stock Fraud</i>	615
	11.2.17 <i>Example 17: Business Liability through Misuse of Organization's Information Processing Assets</i>	617
	11.2.18 <i>Example 18: Parliament Attack</i>	617
	11.2.19 <i>Example 19: Game Source Code Stolen!</i>	617
	11.2.20 <i>Example 20: The Petrol Pump Fraud</i>	618
	11.2.21 <i>Example 21: Xiao Chung's Story – Life of a Hacker</i>	618

11.2.22 <i>Example 22: Killers Take Tips from 26/11 Attack to Use VOIP</i>	621
11.2.23 <i>Example 23: "Robberson" Brothers Caught for Selling Pirated Software</i>	622
11.2.24 <i>Example 24: BSA Uncovers Software IPR Breaches</i>	622
11.2.25 <i>Example 25: Pune City Police Bust Nigerian Racket</i>	623
11.3 Mini-Cases	624
11.3.1 <i>Mini-Case 1: Cyberpornography Involving a Juvenile Criminal</i>	625
11.3.2 <i>Mini-Case 2: Indian Cyberdefamation Case of a Young Couple</i>	625
11.3.3 <i>Mini-Case 3: The Zyg-Zigler Case</i>	626
11.3.4 <i>Mini-Case 4: Internet Time Stealing</i>	627
11.3.5 <i>Mini-Case 5: New York Times Company vs. Sullivan Case of Cyberdefamation</i>	627
11.3.6 <i>Mini-Case 6: The Indian Case of Online Gambling</i>	628
11.3.7 <i>Mini-Case 7: An Indian Case of Intellectual Property Crime</i>	629
11.3.8 <i>Mini-Case 8: The Slumdog Millionaire Movie Piracy Case</i>	629
11.3.9 <i>Mini-Case 9: Malicious Hacking Case – Organ Donation Database Deleted</i>	630
11.3.10 <i>Mini-Case 10: The Case of Counterfeit Computer Hardware</i>	631
11.3.11 <i>Mini-Case 11: The Chinese Case of Trade Secret Stealing Involving an E-Waste Company</i>	631
11.3.12 <i>Mini-Case 12: Internet Used for Murdering</i>	632
11.3.13 <i>Mini-Case 13: Social Networking Victim – MySpace Suicide Case</i>	632
11.3.14 <i>Mini-Case 14: State of Tamil Nadu vs. Suhas Katti Case</i>	633
11.3.15 <i>Mini-Case 15: Pune Citibank MphasiS Call Center Fraud</i>	634
11.3.16 <i>Mini-Case 16: NASSCOM vs. Ajay Sood and Others</i>	635
11.3.17 <i>Mini-Case 17: Indian Case of Cyberdefamation</i>	636
11.3.18 <i>Mini-Case 18: Indian Cases of Cybersquatting</i>	637
11.3.19 <i>Mini-Case 19: Swedish Case of Hacking and Theft of Trade Secrets</i>	640
11.3.20 <i>Mini-Case 20: IPR Violation</i>	640
11.3.21 <i>Mini-Case 21: Indian E-Mail Spoofing Case</i>	641
11.4 Illustrations of Financial Frauds in Cyber Domain	641
11.4.1 <i>Banking-Related Frauds</i>	641
11.4.2 <i>Credit Card-Related Frauds</i>	644
11.4.3 <i>Other Illustrations</i>	655
11.5 Digital Signature-Related Crime Scenarios	661
11.5.1 <i>Part I: Offenses Under the Indian IT Act</i>	661
11.5.2 <i>Part II: Fake/Inaccurate Data in Certificates from Public Certifying Authorities</i>	665
11.6 Digital Forensics Case Illustrations	668
11.6.1 <i>Digital Forensics Illustration 1: Confidential Data Theft Revealed through Forensics Investigation</i>	669
11.6.2 <i>Digital Forensics Case Illustration 2: Analysis of Seized Floppy – the Drug Peddler Case</i>	680

	11.6.3 <i>Digital Forensics Reporting Illustration 1: Vehicle Stealing Racket Revealed through Computer Forensics Investigation</i>	705
	11.6.4 <i>Digital Forensics Reporting Illustration 2: Child Pornography Revealed through Computer Repair</i>	708
11.7	Online Scams	711
	11.7.1 <i>Scam No. 1 – Foreign Country Visit Bait</i>	712
	11.7.2 <i>Scam No. 2 – Follow-up scamming</i>	713
	11.7.3 <i>Scam No. 3 – Purchasing Goods and Services Scam</i>	713
	11.7.4 <i>Scam No. 4 – Cheque Cashing Scam</i>	714
	11.7.5 <i>Scam No. 5 – Romance Scam</i>	714
	11.7.6 <i>Scam No. 6 – Lottery Scam</i>	715
	11.7.7 <i>Scam No. 7 – The Hitman Scam</i>	716
	11.7.8 <i>Scam No. 8 – Bomb Scams</i>	716
	11.7.9 <i>Scam No. 9 – Charity Scams</i>	716
	11.7.10 <i>Scam No. 10 – Fraud Recovery Scams</i>	717
	11.7.11 <i>Scam No. 11 – Pet Scams</i>	717
	11.7.12 <i>Scam No. 12 – Bona Vacantia Scam</i>	718
	11.7.13 <i>Scam No. 13 – Fake Job Offer Scams</i>	719
	11.7.14 <i>Scam No. 14 – Rent Scams</i>	723
	11.7.15 <i>Scam No. 15 – Attorney Debt Collection Scams</i>	725
	11.7.16 <i>Scam No. 16 – Malware Scams</i>	726
	11.7.17 <i>Scam No. 17 – The Advance Fee Fraud</i>	728
	11.7.18 <i>Scam No. 18 – Babysitting Scams</i>	733
	11.7.19 <i>Scam No. 19 – Nigerian 419 Scam</i>	738
	11.7.20 <i>Scam No. 20 – Craigslist Scams</i>	740
	11.7.21 <i>Scam No. 21 – Pyramid Scheme Scams and Ponzi Scheme Scams</i>	741
	Further Reading	743
12	Careers in Cybersecurity	751
	Learning Objectives	751
12.1	Introduction	751
12.2	IT Security Organization	754
	12.2.1 <i>Roles and Responsibilities</i>	754
12.3	Career Paths in Cybersecurity	759
	12.3.1 <i>Assurance and Compliance Security Audit</i>	759
	12.3.2 <i>Types of Assurance and Compliance</i>	760
	12.3.3 <i>Network Security</i>	761
	12.3.4 <i>Cybercrime Investigation and Litigation</i>	761
	12.3.5 <i>Computer Forensics</i>	761
12.4	Cybersecurity Certifications	762
	12.4.1 <i>Classification of Certifications</i>	762
12.5	Guide Path	767
	Summary	771
	References	772
	Further Reading	772



Appendices in CD

Appendix A	Glossary of Cybersecurity Terms and Acronyms
Appendix B	List of Useful Software Utilities and Websites
Appendix C	E-Mail Security and Etiquettes and Policy Template for Computer and Network Usage
Appendix D	Protection Checklist for Individuals and Organizations Template
Appendix E	List of Tools: Vulnerability Scanning and Penetration Testing
Appendix F	Guidelines for Computer Forensics Laboratory Set-up and Guidance on Forensic Readiness Activities in Organizations
Appendix G	Preservation of Digital Crime Scene Related Photographs and Checklist for Processing Computer Forensic Data and Evidence
Appendix H	Guidance on Structuring the Incidence Response Handling Team
Appendix I	List of Forensic Equipment and Forensic Software Tools
Appendix J	Cybercafe Due Diligence Questionnaire
Appendix K	Virtual Crime
Appendix L	Cybercrimes Worldwide – Trends and Patterns
Appendix M	Data Privacy, Data Protection and Cybercrime
Appendix N	Digital Rights Management
Appendix O	The Indian Information Technology Act
Appendix P	The Indian Penal Code
Appendix Q	The Indian Evidence Act
Appendix R	The Indian Patents Act
Appendix S	The Indian Trademarks Act
Appendix T	The Indian Copyright Act
Appendix U	DSCI Security Framework (DSF) from Data Security Council of India
Appendix V	DSCI Privacy Framework (DPF) from Data Security Council of India
Appendix W	Chapterwise List of All References

List of Figures

Figure 1.1	Cybercrime trend.	4
Figure 1.2	Rise in the number of Phishing hosts.	13
Figure 1.3	How a zombie works.	14
Figure 1.4	Major types of incidents by percentage.	16
Figure 1.5	Anonymity for Internet users.	20
Figure 1.6	Twitter site hacked.	24
Figure 1.7	Pentagon, the US site defaced.	24
Figure 1.8	Octomom's defaced website.	25
Figure 1.9	Department of justice site defaced.	26
Figure 1.10	CIA (Central Intelligence Agency), the US, website defaced.	26
Figure 1.11	Dollars lost (year 2008) due to (software) piracy – regional scenario.	29
Figure 1.12	Regional picture on piracy rate.	29
Figure 1.13	Worldwide picture on anti-Spam legislation.	37
Figure 1.14	Extended enterprise.	38
Figure 2.1	We all vouch for keeping your personal information secret!	46
Figure 2.2	Network vulnerabilities – sample network.	47
Figure 2.3	Social engineering – shoulder surfing.	63
Figure 2.4	Sending fake E-Mails.	64
Figure 2.5	Cybercafe security.	70
Figure 2.6	Virtual keyboard.	70
Figure 2.7	Security warnings.	71
Figure 2.8	Botnets are used for gainful purposes.	72
Figure 3.1	Typical hand-held devices.	82
Figure 3.2	Mobile, wireless and hand-held devices.	83
Figure 3.3	Mobility types and implications.	84
Figure 3.4	Online environment for credit card transactions.	87
Figure 3.5	Closed-loop environment for wireless (CLEW).	89
Figure 3.6	Important issues for managing mobile devices.	91
Figure 3.7	Registry value browsing.	92
Figure 3.8	Push attack on mobile devices. DDoS implies distributed denial-of-service attack.	94
Figure 3.9	Pull attack on mobile devices.	95
Figure 3.10	Crash attack on mobile devices. DoS – Denial-of-service attack.	96
Figure 3.11	Communication from mobile client to organization information store.	97
Figure 3.12	Unconventional/stealth storage devices.	109
Figure 3.13	Most important management or support issues for laptops.	112
Figure 3.14	(a) Kensington cable locks for laptops. (b) Closer view of cable locks for laptops.	118

Figure 3.15	Laptop alarm systems with sensors.	119
Figure 4.1	Virus spreads through the Internet.	143
Figure 4.2	Virus spreads through stand-alone system.	144
Figure 4.3	Virus spreads through local networks.	144
Figure 4.4	How steganography works.	156
Figure 4.5	Denial-of-service (DoS) attack.	160
Figure 4.6	Wireless networks.	172
Figure 5.1	Phishing attack – flowchart.	205
Figure 5.2	Medical domain – interconnected entities.	216
Figure 6.1	A cybersecurity perspective: European Union.	228
Figure 6.2	Opt-In and Opt-Out.	236
Figure 6.3	Relationships among supranational European organizations.	248
Figure 6.4	Cybercrime laws: Extent of progress on updating.	307
Figure 6.5	Countries with updated laws.	308
Figure 7.1	Data seen using forensics tools. FAT means file allocation table.	322
Figure 7.2	Hidden and miniaturized storage media.	326
Figure 7.3	Path of the digital evidence.	330
Figure 7.4	Bottom-up approach to tracing E-Mail source.	335
Figure 7.5	Process model for understanding a seizure and handling of forensics evidence legal framework.	340
Figure 7.6	Media that can hold digital evidences.	343
Figure 7.7	Some more media that can hold digital evidences.	344
Figure 7.8	Embedded memories inside computer. (a) Read-only memory (ROM) chips; (b) erasable programmable read-only memory (EPROM) chip; (c) programmable read-only memory (PROM) chips; (d) electrify erasable programmable read-only memory (EEPROM) chips.	345
Figure 7.9	An image constructed from a fragmented file.	348
Figure 7.10	Maintaining chain of custody – 1.	356
Figure 7.11	Maintaining chain of custody – 2. (a) Source of evidence – where did it come from? (b) Who found it? (c) Where was it stored/locked up? (d) Who touched it/tampered with it? (e) What did they do to it? What did they do with it? (f) Human signature is always required.	356
Figure 7.12	Cyberforensics laboratory – 1.	362
Figure 7.13	Cyberforensics laboratory – 2.	363
Figure 7.14	Cyberforensics equipments.	363
Figure 7.15	Connectors used with cyberforensics tools.	364
Figure 7.16	Disk duplication equipment in a forensics laboratory.	365
Figure 7.17	Portable forensics kits.	366
Figure 7.18	FastBloc – the Field Kit and the Lab Kit. (a) The lab edition and (b) the field edition.	366
Figure 7.19	(a) SIM card reader, (b) iButtons, (c) flash memory, (d) SIM card.	367
Figure 7.20	The OSI 7 Layer Model with Internet Protocols.	374

Figure 7.21	Network hacking steps.	374
Figure 7.22	Hacker categories (profit and damage).	375
Figure 7.23	User concerns about privacy on social networking sites (LinkedIn, Facebook, WoW).	379
Figure 7.24	Privacy concerns about social networking sites vary with age.	379
Figure 7.25	On the Internet, it does not matter “who” you are as long as you have “ID”!!	382
Figure 7.26	Traditional approach to forensics analysis.	387
Figure 8.1	Hand-held devices. (a) iPhone; (b) iPod; (c) palm pilot; (d) digital diary; (e) Smartphones; (f) 2 GB MP2 player; (g) portable printer; (h) handycam and (i) PDA.	424
Figure 8.2	Faraday bags.	429
Figure 8.3	Smartphones market is growing even when general mobile phones market is falling.	442
Figure 8.4	Logical analysis of Smartphones.	444
Figure 8.5	iPhone tear-down image: top view.	446
Figure 8.6	iPhone tear-down image: bottom view.	447
Figure 8.7	Device information screen.	448
Figure 8.8	Information examiner screen.	449
Figure 8.9	Device seizure wizard screen.	449
Figure 8.10	Device selection screen.	450
Figure 8.11	Summary of selections screen.	451
Figure 8.12	Acquisition process screen.	451
Figure 8.13	Digital photographs and images examples. (a) Type of note taking image that is used as an illustration of the shirt examined, (b) record image of a firearm which is generally used for court purposes, (c) typical image (finger mark) used for Biometric comparison, (d) intelligence image in which shoe-mark image provides information about the make and model of the shoe, (e) a CCTV image.	455
Figure 8.14	Digital image adjustment example.	456
Figure 8.15	Bullet trajectory mapping example.	456
Figure 8.16	BlackBerry unit's control functions – set 1. (a) Radio status control and (b) device status control.	461
Figure 8.17	BlackBerry unit's control functions – set 2. (a) Battery status, (b) CPU WatchPuppy and (c) file memory status.	462
Figure 8.18	BlackBerry unit's control functions – set 3. (a) Common port and (b) file system.	463
Figure 8.19	BlackBerry unit's control functions – set 4. (a) OTA status function and (b) halt and reset status function.	463
Figure 8.20	Example – PDA data acquired using a PDA seizure toolkit.	465
Figure 8.21	Apple iPods. (a) Apple iPOD (regular), (b) Apple iPOD (mini), (c) Apple iPOD (fourth generation) and (d) Apple iPOD (nanochromatic series).	468
Figure 8.22	Antistatic bags for handling digital evidence.	473
Figure 9.1	A cybersecurity perspective.	496

Figure 9.2	Insider threat scenario (2000–2009).	497
Figure 9.3	Cybercrimes – the flow and connections.	499
Figure 9.4	Security threats – paradigm shift.	500
Figure 9.5	Cost of cybercrimes.	501
Figure 9.6	Probabilities of system failure (use of pirated software).	505
Figure 9.7	Policy hierarchy chart.	509
Figure 9.8	Social media – online tools.	517
Figure 9.9	Firewall with DMZ networks.	521
Figure 9.10	Anonymity by web proxy.	525
Figure 9.11	Incident response, incident handling and incident management – the relationship.	532
Figure 9.12	Entities involved in incident-related actions and communication.	533
Figure 9.13	Threats, vulnerabilities, assets and risks.	536
Figure 9.14	Incident management and security management.	538
Figure 9.15	Statistics – incidents handled by CERT-In (categories).	540
Figure 9.16	Incident response life cycle.	544
Figure 9.17	Process flow: Incident response management system.	546
Figure 9.18	Cyberforensics and case investigation: Where it ends.	549
Figure 9.19	The path to compromise an asset.	555
Figure 9.20	Access management framework – key elements.	558
Figure 9.21	Security throughout SDLC.	564
Figure 10.1	Ethics in computing.	572
Figure 10.2	Contexts for professional ethics.	580
Figure 10.3	Hackers' motives (profit and damage).	583
Figure 10.4	Cybercrimes – the connections and syndicates.	584
Figure 10.5	Hackers community.	585
Figure 10.6	Sophistication of hacker attacks.	588
Figure 10.7	Hacker technical skills continuum.	589
Figure 10.8	Cybercrimes are boundary-less!	595
Figure 11.1	Cybercrimes are boundary less!	604
Figure 11.2	Maharashtra state website hacked.	606
Figure 11.3	The young hacker at work.	619
Figure 11.4	Fate of cybercrime cases (total cases-to-sentenced cases).	644
Figure 11.5	Entities involved in credit card transactions.	645
Figure 11.6	Credit card fraud classification.	646
Figure 11.7	Man-in-the-middle attack.	647
Figure 11.8	Credit card skimmer devices.	650
Figure 11.9	Credit card security code.	651
Figure 11.10	Credit card swiping machine.	652
Figure 11.11	Hackers' motives and goals.	654
Figure 11.12	Spoofed chase site.	667
Figure 11.13	Site with misleading organization name.	668
Figure 11.14	GUI enhancement.	668
Figure 11.15	Employee getting performance appraisal mail.	670
Figure 11.16	Employee receives mail from competitor organization.	670

Figure 11.17	Employee reading a malicious program instructions.	671
Figure 11.18	Ex-organization's employee reading the mail containing malicious attachment.	671
Figure 11.19	Donation request mail planted as bait by the revengeful employee.	672
Figure 11.20	Suspect employee's desktop.	672
Figure 11.21	The data dump from suspect employee machine.	673
Figure 11.22	The cracked account.	674
Figure 11.23	The tagged document.	675
Figure 11.24	The hex dumps.	675
Figure 11.25	Trail on the forensically cracked account.	676
Figure 11.26	"Cleaning" the tracks act.	676
Figure 11.27	Digital evidence recovery-1.	677
Figure 11.28	The digital evidence recovery-2.	677
Figure 11.29	The digital evidence recovery-3.	678
Figure 11.30	More evidence.	678
Figure 11.31	Case report from the forensics tool-1.	679
Figure 11.32	Case screen from the forensics tool-2.	679
Figure 11.33	Evidence on the hard disk.	680
Figure 11.34	Autopsy case creation.	682
Figure 11.35	Autopsy new case creation.	683
Figure 11.36	Autopsy: Case study created.	683
Figure 11.37	Autopsy: New host added.	684
Figure 11.38	Autopsy: Host "floppyhost" added.	685
Figure 11.39	Autopsy: Case and host info added.	685
Figure 11.40	Autopsy: New image added.	686
Figure 11.41	Autopsy: Image type.	686
Figure 11.42	Autopsy: Image file details.	687
Figure 11.43	Autopsy – Image File Details (upper) and Host Manager Details (lower).	688
Figure 11.44	Autopsy: String details.	688
Figure 11.45	Autopsy: Image details (extracting strings).	689
Figure 11.46	Autopsy: Image details after extracting strings.	690
Figure 11.47	Autopsy: The result of extracting unallocated sectors.	690
Figure 11.48	Autopsy: Image details after the extraction of unallocated sectors.	691
Figure 11.49	Autopsy: Result of extracting strings from unallocated sectors.	691
Figure 11.50	Autopsy: Image details of extraction of allocated and unallocated strings.	692
Figure 11.51	Autopsy: File analysis mode.	692
Figure 11.52	Autopsy: File analysis – "cover page.jpgc" – ASCII display.	693
Figure 11.53	Autopsy: Metadata Analysis – ASCII display "cover page.jpgc".	694
Figure 11.54	Autopsy: keyword search – JFIF.	694
Figure 11.55	Autopsy: Result of keyword search – JFIF.	695
Figure 11.56	Autopsy: Data unit analysis.	695

xxxviii List of Figures

Figure 11.57	Autopsy: Data unit analysis – allocation list.	696
Figure 11.58	Autopsy: Data unit analysis – export contents option.	697
Figure 11.59	Image contained in “coverpage.jpg” file.	698
Figure 11.60	Autopsy: File analysis – ASCII display of the file “Jaggu Jungle.doc”.	698
Figure 11.61	Autopsy: Metadata analysis of the file “Jaggu Jungle.doc”.	699
Figure 11.62	Disk structure.	700
Figure 11.63	Autopsy: File analysis – ASCII display of “Scheduled Visits.exe”.	701
Figure 11.64	Autopsy: File analysis – metadata analysis of “Scheduled Visits.exe”.	701
Figure 11.65	TDD device.	732
Figure 12.1	CIA triad.	752
Figure 12.2	Types of personal information in organizations.	752
Figure 12.3	IT security organization chart.	755

List of Tables

Table 1.1	Cybercrimes/cases registered and persons arrested under IT Act during 2004–2007	5
Table 1.2	Cybercrimes/cases registered and persons arrested under IPC during 2004–2007	6
Table 1.3	2005 Cases under cybercrime – part A	7
Table 1.4	2005 Cases under cybercrime – part B	10
Table 1.5	Cybercrime trend over the years (1999–2008)	15
Table 1.6	Classifying cybercrimes – broad and narrow	17
Table 1.7	The key provisions under the Indian ITA 2000 (before the amendment)	34
Table 2.1	Tools used during passive attacks	52
Table 2.2	Tools used during active attacks	54
Table 2.3	Well-known port numbers	59
Table 2.4	Cloud computing service providers	76
Table 2.5	Risks associated with cloud computing environment	78
Table 3.1	Bluetooth hacking tools	106
Table 4.1	Websites and tools used to find the common vulnerabilities	127
Table 4.2	Tools used to cover tracks	128
Table 4.3	Password cracking tools	133
Table 4.4	Types of password cracking attacks	135
Table 4.5	Software keyloggers	138
Table 4.6	Spywares	141
Table 4.7	Difference between computer virus and worm	145
Table 4.8	The world's worst virus attacks!!!	147
Table 4.9	The world's worst virus and worm attacks!!!	149
Table 4.10	Steganography tools	157
Table 4.11	Steganalysis tools	158
Table 4.12	Classification of DoS attacks	159
Table 4.13	Tools used to launch DoS attack	161
Table 4.14	Tools used to launch DDoS attack	163
Table 4.15	Tools for detecting DoS/DDoS attacks	164
Table 4.16	Tools used for SQL Server penetration	166
Table 4.17	Tools used to defend/protect buffer overflow	171
Table 4.18	Tools used for hacking wireless networks	176
Table 4.19	Tools to protect wireless network	180
Table 5.1	How to avoid being victim of Phishing attack	202
Table 5.2	Anti-Phishing plug-ins	205
Table 5.3	Myths and facts about identity theft	208
Table 5.4	Business identity theft – countermeasures	214
Table 5.5	How to prevent being victim of identity theft	220

Table 5.6	How to protect/efface your online identity	221
Table 6.1	Asia-Pacific region: Alignment of the countries enacted legislation with regard to the benchmark legislation	235
Table 6.2	Asia-Pacific region: Alignment of the countries enacted legislation with regard to Microsoft Model Privacy Bill	236
Table 6.3	Asia-Pacific region: Alignment of the countries enacted legislation with regard to anti-Spam laws (Microsoft checklist)	241
Table 6.4	Asia-Pacific region: Alignment of the countries enacted legislation with regard to European Cybercrime Convention and ICMEC's Model Child Pornography Legislation	242
Table 6.5	Cybercrime legislation in some of the African countries	251
Table 6.6	The Indian ITA 2000: Summary of contents (main elements only)	255
Table 6.7	Summary of changes to the Indian IT Act (significant changes brought out by the IT Amendment Bill 2008)	260
Table 6.8	ITA 2008 and cybercafes	290
Table 6.9	ITA 2008 and Indian IT and ITES companies	296
Table 7.1	E-Mail header example	333
Table 7.2	Typical E-Mail header	336
Table 7.3	Header of a fake mail (an example only)	337
Table 7.4	E-Mail header with several identifiers	338
Table 7.5	Digital forensics – phase-wise outputs	353
Table 7.6	Top 10 social networking sites (year 2009) – security features	380
Table 7.7	Top 10 social networking sites (year 2010) – security features	381
Table 7.8	Retrieving sender's IP address from E-Mail received	382
Table 7.9	List of carving tools	397
Table 7.10	Forensics tools features comparison at a glance	400
Table 7.11	Top tools in digital forensics	401
Table 8.1	Hardware characteristics: Hand-held devices	430
Table 8.2	Software characteristics: Hand-held devices	431
Table 8.3	Cell phone tools and SIM tools	435
Table 8.4	PDA forensics tools	439
Table 8.5	iPhone hardware components	445
Table 8.6	iPhone forensics: Sample list of test cases	452
Table 8.7	E-Discovery and computer forensics: The difference	476
Table 8.8	Cell phone forensics – Organizational guidelines	485
Table 9.1	Business area-wise information	520
Table 9.2	Cybersecurity incident examples	539
Table 9.3	Summary of cybersecurity incidents handled by CERT-In	540
Table 9.4	Incident response process – phases/components	542
Table 9.5	Diagnostic matrix example	545
Table 9.6	Forensics readiness – organizational concerns	552
Table 9.7	Information assets – the three key dimensions for protection prioritization	556
Table 9.8	Endpoint security – important touch points	562

Table 11.1	List of examples in Section 11.2	605
Table 11.2	List of Mini-Cases in Section 11.3	624
Table 11.3	List of illustrations in Section 11.4	642
Table 11.4	List of illustrations in Section 11.5	661
Table 11.5	Cybercrimes punishment (partial reproduction of Table 1.7 of Chapter 1)	663
Table 11.6	Illustrations in Section 11.6	669
Table 11.7	Sector allocations (digital forensics using Autopsy Tool Kit)	696
Table 11.8	File contents – “Scheduled Visits.xls”	702
Table 11.9	Answers to the case questions	704
Table 11.10	The primary report (1)	705
Table 11.11	The primary report (2)	709
Table 11.12	Case brief report	710
Table 11.13	Scams described in Section 11.7	712
Table 11.14	Beware of rent scammers	724
Table 12.1	Information security-related certifications	763
Table 12.2	List of important certifications	764
Table 12.3	Guide path: Assurance and compliance security audits	768
Table 12.4	Guide path: Network security	768
Table 12.5	Guide path: Cybercrime investigation and litigation	769
Table 12.6	Guide path: Computer forensics	770

List of Boxes

Box 1.1	Cyberspace, Cybersquatting, Cyberpunk, Cyberwarfare and Cyberterrorism	2
Box 1.2	The Botnet Menace!	14
Box 1.3	Internet: A New Fuel for Defamation?	20
Box 1.4	The Story of a Hacked Website	25
Box 1.5	Spam in Cyberworld	31
Box 1.6	Cybercrimes: Indian Statistics	33
Box 1.7	Hacking and the ITA 2008	35
Box 2.1	Hackers, Crackers, and Phreakers	46
Box 2.2	What Color is Your Hat in the Security World?	47
Box 2.3	Patriot Hacking	49
Box 2.4	Tips for Effective Search with “Google” Search Engine	50
Box 2.5	Ports and Ports Scanning	58
Box 2.6	Social Engineering Example	62
Box 2.7	Fake E-Mails	64
Box 2.8	Cyberbullying	67
Box 2.9	Explanation for Technical Terms used in Fig. 2.8	72
Box 2.10	Zero-Day Attack	74
Box 3.1	Key Findings for Mobile Computing Security Scenario	85
Box 3.2	Tips to Prevent Credit Card Frauds	88
Box 3.3	Potential Wireless Users – Beware!	89
Box 3.4	LDAP Directory Structure	96
Box 3.5	RAS System Security for Mobile Device Clients	97
Box 3.6	Tips to Secure your Cell/Mobile Phone from being Stolen/Lost	99
Box 3.7	Pretexting, Sexting and VoIP Spam	103
Box 3.8	SMS Blocker	105
Box 3.9	Bluetooth	105
Box 3.10	Hacking Mobile Phones	107
Box 3.11	TrustZone Technology for Mobile Devices – Toward Security of M-Commerce Applications	108
Box 3.12	Getting Lost!!	111
Box 3.13	Spy Phone Software!!!	116
Box 4.1	Scareware, Malvertising, Clickjacking and Ransomware	126
Box 4.2	Being Anonymous While Searching on Google!	130
Box 4.3	Malwares	141
Box 4.4	More about Viruses!	147
Box 4.5	Trojan War	151
Box 4.6	Peer-to-Peer (P2P) Networks	154
Box 4.7	Difference between Steganography and Cryptography	156
Box 4.8	Blended Threat	162
Box 4.9	Permanent Denial-of-Service (PDoS) Attack	162

Box 4.10	Going Wi-Fi	173
Box 4.11	The New “Wars” in the Internet Era!	178
Box 5.1	APWG (Anti-Phishing Working Group)	186
Box 5.2	SPAMBOTS	188
Box 5.3	CAN-SPAM Act	188
Box 5.4	Website Spoofing, XSS and XSRF	191
Box 5.5	Phishing vis-à-vis Spoofing	192
Box 5.6	Homograph Attack	194
Box 5.7	Phishing Attack Launched through Android Market	194
Box 5.8	Avoiding Spear Phishing Scams	196
Box 5.9	Advanced Form of Phishing – Tabnapping or Tabjacking	197
Box 5.10	Three Ps of Cybercrime – Phishing, Pharming and Phoraging	198
Box 5.11	DNS Hijacking and Click Fraud	198
Box 5.12	SEO Attacks – Beware While Searching through Search Engines!	200
Box 5.13	How to Judge/Recognize Legitimate Websites	204
Box 5.14	Identity Theft Resource Center (ITRC)	207
Box 5.15	Chinese Ghost Net	213
Box 5.16	HIPAA, PHI and HITECH	217
Box 5.17	Geotagging	219
Box 6.1	Degrees of Unlawful Access to Computer	229
Box 6.2	The APEC Framework on Privacy	233
Box 6.3	India and Anti-Spam Legislation	239
Box 6.4	PIPEDA – The Canadian Act for Protecting Personal Information	243
Box 6.5	ECPA: The New Dawn in Canadian Legislation	244
Box 6.6	The Florida Computer Crimes Act	246
Box 6.7	The EU Member Countries	247
Box 6.8	The European Data Protection Directive	248
Box 6.9	The European Convention on Cybercrime	250
Box 6.10	Cybercrimes and Other Related Crimes Punishable under Indian Laws	254
Box 6.11	Data Protection and the New Clause 43A under the Amended IT Act	259
Box 6.12	Digital Evidence and its Admissibility in Courts	263
Box 6.13	X.509 Digital Certificates	274
Box 6.14	ITA 2000 Oversight	274
Box 6.15	Digital Signature and Public-Key Infrastructure Technology	276
Box 6.16	PKI – Basic Components	276
Box 6.17	EDIFACT Basics	280
Box 6.18	HIPAA-HITECH – Data Protection Implications for the Healthcare Industry	300
Box 6.19	The EU Contract Clause – Understanding the Entities and Implications	301
Box 7.1	COFEE Time!	320
Box 7.2	Differences between Forensics Policy and Security Policy	322
Box 7.3	Digital Forensics Investigations and E-Discovery	323
Box 7.4	Chain of Custody Example	326

Box 7.5	The Father of Forensics Science – the Sherlock Holmes of France	328
Box 7.6	Electronic Messages and the Indian Evidence Act	332
Box 7.7	Points to Remember when you Use E-Mail as an Evidence	334
Box 7.8	Forensics Experts – What do they Do?	341
Box 7.9	Case Briefings	342
Box 7.10	File Carving – a Powerful Tool for Digital Forensics	347
Box 7.11	The RAID Levels	350
Box 7.12	The Chain of Evidence Concept	356
Box 7.13	Steganography, Cryptography and Digital Watermarks	369
Box 7.14	Hair Splitting Experience for Forensics	
	Investigation Experts!	371
Box 7.15	Hide and Seek in the World of Information Communication	372
Box 7.16	California Senate Bill 1386 (Another Angle to Cyberforensics)	384
Box 7.17	Drama in Court! Impact of Cyberforensics	
	on Legal Practitioners	394
Box 7.18	Beware – Forensics Act and Laws!	395
Box 7.19	Auditing vis-à-vis Cyberforensics Investigation	404
Box 8.1	CDMA, TDMA, GSM, AMPS and DoCoMo and Other Standards	426
Box 8.2	Mobile Handsets Challenges – Tracing Call Logs	
	and Retrieving Information	428
Box 8.3	Hand-Held Devices and Digital Forensics	432
Box 8.4	Cell Phone – Smart Tips	434
Box 8.5	“Jailbroken” Devices!!	450
Box 8.6	iPod Forensics – Legal Considerations	470
Box 8.7	SMART Forensics Tools	478
Box 9.1	Mobile Workforce – Category of “Remote Workers”	506
Box 9.2	Cookies and Internet Activities	508
Box 9.3	Cookies – Where Did They Come From?	510
Box 9.4	Cookies and Fair Information Practices to Avoid Privacy Loss	510
Box 9.5	Organizations Have the Choice: Proactive vs.	
	Reactive Approach to Security	512
Box 9.6	Protecting Your Online Privacy – You may be “Fingered”!	523
Box 9.7	Anonymizers: The Boon and the Bane!	524
Box 9.8	Malware Incidents	539
Box 9.9	Be Careful with E-Mail and Attachments	559
Box 10.1	The Philosophy Behind Copyrights	575
Box 10.2	Copy Protection with DRM – Digital Rights Management	576
Box 10.3	Cybersquatting and Trademarks	579
Box 10.4	Ethics and Morality	581
Box 10.5	Computer Ethics	583
Box 10.6	Understanding Ethical Hacking	590
Box 10.7	The Hacktivist	591
Box 10.8	Information Warfare Classification	594
Box 10.9	Privacy on the Internet and TOR	596
Box 12.1	CSO Magazine	757
Box 12.2	Certification Magazine	762

1 | Introduction to Cybercrime

Learning Objectives

After reading this chapter, you will able to:

- Learn what cybercrime is and appreciate the importance of cybercrime as the topic.
 - Understand the different types of cybercrime.
 - Understand the difference between cybercrime and cyberfraud.
 - Learn about different types of cybercriminals and the motives behind them.
 - Get an overview of cybercrime scenario in India as well as the overall global perspective.
 - Understand the legal perspective on cybercrime including the Indian ITA 2000 and its latest amendment known as the ITA 2008.
-

1.1 Introduction

Almost everyone is aware of the phenomenal growth of the Internet (the statistics on Indian growth for Internet and mobile usage are indicated through links provided in Ref. #26, Additional Useful Web References, Further Reading). Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime. These activities involve the use of computers, the Internet, cyberspace (see Box 1.1) and the worldwide web (WWW). Interestingly, cybercrime is *not* a new phenomena; the first recorded cybercrime took place in the year 1820. It is one of the most talked about topics in the recent years. Figure 1.1, based on a 2008 survey in Australia, shows the cybercrime trend. Also refer to Appendix L.

While the worldwide scenario on cybercrime looks bleak, the situation in India is not any better. Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002. There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009 (see Ref. #2, Articles and Research Papers, Further Reading).

Similar data for later years is presented in Tables 1.1–1.4; the data in those tables show statistics related to various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

1.2 Cybercrime: Definition and Origins of the Word

With the backdrop of information in the previous section and the statistics presented in Tables 1.1 and 1.2, let us understand the origins of the term *cybercrime*. Reaching consensus on a definition of computer

Box 1.1

Cyberspace, Cybersquatting, Cyberpunk, Cyberwarfare and Cyberterrorism

Cyberspace

This is a term coined by William Gibson, a science fiction writer, in his Sci-fi novel *Neuromancer* (published in 1984) – he suggested it as a “consensual hallucination.” According to his vision about near-future computer network (as at the time when he coined the term in 1984), “cyberspace” is where users mentally travel through matrices of data. Conceptually, “cyberspace” is the “nebulous place” where humans interact over computer networks. The term “cyberspace” is now used to describe the Internet and other computer networks. In terms of computer science, “cyberspace” is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data. A common factor in almost all definitions of cyberspace is the sense of place that they convey – cyberspace is most definitely a place where you chat, explore, research and play.

Cybersquatting

The term is derived from “squatting” which is the act of occupying an abandoned/unoccupied space/building that the squatter does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process. Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them. This term is explained here because, in a way, it relates to cybercrime given the intent of cybersquatting. Cybersquatting is the act of registering a popular Internet address, usually a company name, with the intent of selling it to its rightful owner. From an affected individual’s point of view, cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else’s trademark. In this nature, it can be considered to be a type of cybercrime. Cybersquatting is the practice of buying “domain names” that have existing businesses names. In other words, cybersquatting involves the pre-emptive registration of trademarks by third parties as domain names. It is done with the intent to sell those “domain names” to earn profit. Comparing cybersquatting to online extortion, Senator Spencer Abraham, a Michigan Republican, introduced to Congress the Anti-Cybersquatting Consumer Protection Act. This bill, if enacted, would make cybersquatting illegal. Violators would be charged a fine of up to \$300,000. The World Intellectual Property Organization (WIPO) has also outlined anti-cybersquatting tactics, which have been endorsed by Internet Corporation for Assigned Names and Numbers (ICANN). Ironically enough, someone recently registered www.wipo.com in order to sell it back to WIPO for several thousand dollars. Even though legislation has not been enacted, almost all cybersquatting court-case decisions are against cybersquatters. We can see that the topic of “domain name disputes” is closely connected with cybersquatting, because domain name disputes arise largely from the practice of cybersquatting. Such disputes happen because cybersquatters exploit the first-come, first-served nature of the domain name registration system to register names of trademarks, famous people or businesses with which they have no connection. Since registration of domain names is relatively simple, cybersquatters can register numerous examples of such names as domain names. As the holders of these registrations, cybersquatters often then put the domain names up for auction, or offer them for sale directly to the company or person involved, at prices far beyond the cost of registration. Alternatively, they can keep the registration and use the name of the person or business associated with that domain name to attract business for their own sites.

In India, “cybersquatting” is considered to be an “Intellectual Property Right” (IPR) evil (see Ref. #29, Additional Useful Web References, Further Reading). In India, “cybersquatting” is seen to interfere with the “Uniform Dispute Resolution Policy” (a contractual obligation to which all domain name registrants are presently subjected to). It also affects the rights of Indians who have to face charges of “Squatting” in respect of international generic domain names such as dot com, dot org, etc. The terms “trademark” and “intellectual property” are explained in Chapter 10.

Box 1.1 Cyberspace, Cybersquatting, . . . (Continued)

Cyberpunk and Cyberwarfare

According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism." The term "cyberpunk" could mean something like "anarchy via machines" or "machine/computer rebel movement." This word first appeared as the title of a short story "Cyberpunk" by Bruce Bethke, published in science fiction stories magazine, AMAZING, Vol. 57, No. 4, November 1983. It is quite interesting to note that the word was coined in the early spring of 1980, and applied to the "bizarre, hard-edged, high-tech" science fiction emerging in the 1980s. The story is about a bunch of teenage hackers/crackers. The idea behind calling it "cyberpunk" was to invent a new term that will express the juxtaposition of punk attitudes and high technology. For the terms "hackers," "crackers" and others, readers may like to refer to specific pages of the source mentioned at the end of this box. Also refer to Chapter 10.

Cyberwarfare, for many people, means information warriors unleashing vicious attacks against an unsuspecting opponent's computer networks, wreaking havoc and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and cyberterrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population. Cyberattacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare. Information warfare (see Ref. #9, Books, Further Reading) covers a range of activities of which cyberattacks may be the least important.

Cyberterrorism

This term was coined in 1997 by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. However, this narrow definition makes it difficult to identify any instances of cyberterrorism. There is a broad definition stated by Kevin G. Coleman of the Technolytics Institute:

The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives.

There is a lot of misinterpretation in the definition of cyberterrorism, the term consisting of familiar word "cyber" and less familiar word "terrorism." Although "cyber" is the term we can understand (see Section 1.2), the term terrorism is difficult to define. The ambiguity in the definition brings in vagueness in action, as D. Denning pointed in her work saying that "'an E-Mail bomb' may be considered as 'hacktivism' by some and 'cyberterrorism' by others" (for terms such as "activism," "hacktivism" and "cyberterrorism", see Ref #13, Additional Web References, Further Reading). There is a degree of understanding of the meanings of cyberterrorism, either from the popular media, other secondary sources or personal experience; however, the specialists use different definitions. "Cyberterrorism", as well as other contemporary "terrorisms" appear as a mixture of words terrorism and a meaning of an area of application. Barry Collin defined cyberterrorism as the convergence of cybernetics and terrorism. In the same year, Mark Pollitt, special agent for the FBI, offers a working definition:

Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against noncombatant targets by sub national groups or clandestine agents.

We can also define cyberterrorism as: Use of information technology and means by terrorist groups and agents. Refer to Chapter 10.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 11.2, p. 170 and Box 38.12, p. 926), Wiley India.

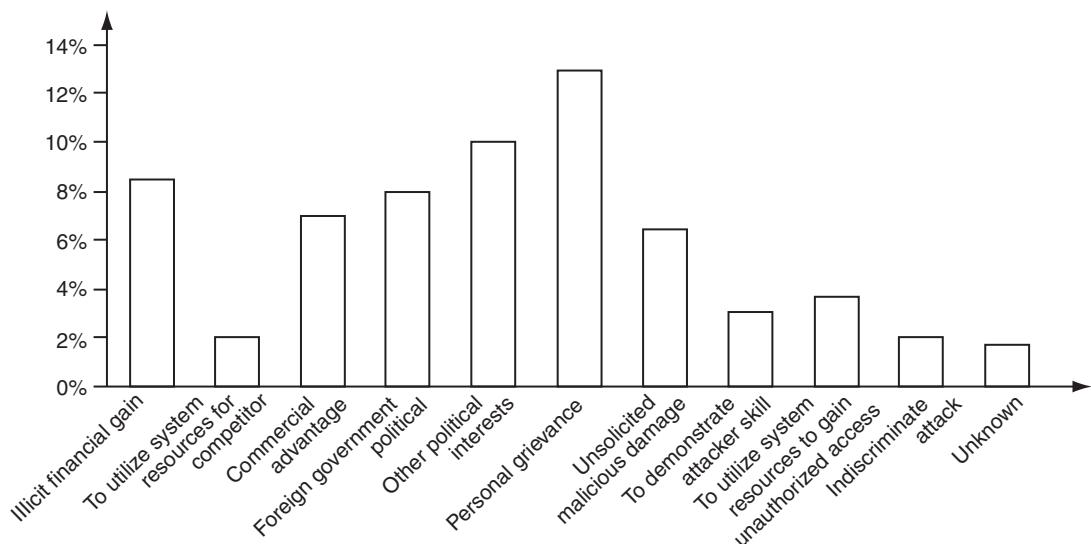


Figure 1.1 | Cybercrime trend.

Source: 2008 Pacific Islands Computer Crime and Security Survey. Adapted from *Cybercrime: Threats, Challenges* presentation by Wipul Jayawickrama at the Computer Security Week 2008 in Brisbane, Australia (reproduced with permission).

crime is difficult. One definition that is advocated is, “*a crime conducted in which a computer was directly and significantly instrumental.*” This definition is not universally accepted. It, however, initiates further discussion to narrow the scope of the definition for “cybercrime”: for example, we can propose the following alternative definitions of computer crime:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. Any financial dishonesty that takes place in a computer environment.
4. Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.

Here is yet another definition: “*cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.*” Note that in a wider sense, “computer-related crime” can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime.

Statute and treaty law both refer to “cybercrime.” The term “cybercrime” relates to a number of other terms that may sometimes be used interchangeably to describe crimes committed using computers. *Computer-related crime, Computer crime, Internet crime, E-crime, High-tech crime*, etc. are the other synonymous terms. Cybercrime specifically can be defined in a number of ways; a few definitions are:

1. A crime committed using a computer and the Internet to steal a person’s identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs. Refer to Chapter 5.

Table 1.1 | Cybercrimes/cases registered and persons arrested under IT Act during 2004–2007

Sr. No.	Crime Heads	Cases Registered			% Variation in 2007 over 2006			Persons Arrested			% Variation in 2007 over 2006		
		2004	2005	2006	2007	2004	2005	2006	2007	2004	2005	2006	2007
1	Tampering computer source documents	2	10	10	11	10.0	0	10	8	2	—	—	—
2	Hacking with computer system	14	33	25	20	-20.0	31	27	34	25	—	-26.5	—
	(i) Loss/damage to computer resource/utility												
3	(ii) Hacking	12	41	34	46	35.3	1	14	29	23	-20.7	6.2	—
	Obscene publication/transmission in electronic form	34	88	69	99	43.5	21	125	81	86	—	—	—
4	Failure	0	1	0	2	—	0	0	0	1	—	—	—
	(i) Of compliance/orders of Certifying Authority												
	(ii) To assist in decrypting the information intercepted by government agency	0	0	0	2	—	0	0	0	0	—	—	—
5	Unauthorized access/attempt to access to protected computer system	0	0	0	4	—	0	0	0	0	—	—	—
6	Obtaining licence or digital signature certificate by misrepresentation/suppression of fact	0	0	0	11	—	0	0	0	11	—	—	—
7	Publishing false digital signature certificate	0	0	0	0	—	0	0	0	0	—	—	—
8	Fraud digital signature certificate	0	1	1	3	200.0	0	3	0	3	—	—	—
9	Breach of confidentiality/privacy	6	3	3	9	200.0	7	13	2	3	50.0	—	—
10	Other	0	0	0	0	—	0	0	0	0	—	—	—
	Total	68	177	142	207	45.8	60	192	154	154	0.0		

Source: <http://www.nasscom.org/download/Cybercrimes in India 2003.pdf> (28 February 2009).

6 Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives

Table 1.2 | Cybercrimes/cases registered and persons arrested under IPC during 2004–2007

Sr. No.	Crime Heads	Cases Registered				% Variation in 2007 over 2006	Persons Arrested				% Variation in 2007 over 2006
		2004	2005	2006	2007		2004	2005	2006	2007	
1	Offences by/ against public servant	0	0	0	0	—	0	0	0	0	—
2	False electronic evidence	0	0	0	0	—	0	0	0	0	—
3	Destruction of electronic evidence	0	0	0	0	—	0	0	0	0	—
4	Forgery	77	48	160	217	35.6	81	71	194	264	36.1
5	Criminal breach of trust/ fraud	173	186	90	73	-18.9	181	215	121	85	-29.8
6	Counterfeiting										
	(i) Property/ mark	12	0	13	8	-38.5	8	0	7	23	228.6
	(ii) Tampering	7	9	0	5	—	16	0	0	8	—
	(iii) Currency/ stamps	10	59	48	36	-25.0	43	82	89	49	-44.9
7	Total	279	302	311	339	9.0	329	368	411	429	4.4

Source: <http://www.nasscom.org/download/Cybercrimes in India 2003.pdf> (28 February 2009).

2. Crimes completed either on or with a computer.
3. Any illegal activity done through the Internet or on the computer.
4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

According to one information security glossary,^[1] cybercrime is any criminal activity which uses network access to commit a criminal act. Opportunities for the exploitation due to weaknesses in information security are multiplying because of the exponential growth of Internet connection (see Ref. #26, Additional Useful Web References, Further Reading). Cybercrime may be internal or external, with the former easier to perpetrate. The term “cybercrime” has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users. *Cybercrime* refers to the act of performing a criminal act using cyberspace as the communications vehicle (the term “cyberspace” is explained in Box 1.1). Some people argue that a cybercrime is not a crime as it is a crime against software and not against a person or property. However, while the legal systems around the world scramble to introduce laws to combat cyber-criminals (refer to Section 1.5), two types of attack are prevalent:

1. **Techno-crime:** A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24 × 7 connection to the Internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, “finger prints.”

Table 1.3 | 2005 Cases under cybercrime – part A
 Cases registered under cybercrimes by motives and suspects during 2005 [States and Union Territories (UTs)]

Sr. No.	State/UT	Motives							Total
		Revenge/ Setting Scores	Greed/ Money	Extortion	Cause Disrepute	Prank/ Satisfaction of Gaining Control	Fraud/Illlegal Gain	Eve Teasing/ Harassment	
<i>States</i>									
1	Andhra Pradesh	0	0	0	0	3	18	3	58
2	Arunachal Pradesh	0	0	0	0	0	0	0	0
3	Assam	0	0	0	0	0	0	1	1
4	Bihar	0	0	0	0	0	0	0	0
5	Chhattisgarh	0	4	0	0	0	1	0	46
6	Goa	0	0	0	0	0	0	1	2
7	Gujarat	0	2	0	1	0	1	0	3
8	Haryana	0	0	0	0	0	1	2	6
9	Himachal Pradesh	0	0	0	0	0	0	0	0
10	Jammu & Kashmir	0	0	0	0	0	0	0	0
11	Jharkhand	0	0	0	0	0	0	0	0
12	Karnataka	4	4	0	3	0	16	10	38
13	Kerala	0	0	0	0	0	0	0	0
14	Madhya Pradesh	0	0	0	0	0	0	0	0
15	Maharashtra	2	4	0	2	1	7	11	0
16	Manipur	0	0	0	0	0	0	0	0
17	Meghalaya	0	0	0	0	0	0	0	0
18	Mizoram	0	0	0	0	0	0	0	0
19	Nagaland	0	0	0	0	0	0	0	0
20	Orissa	0	0	0	0	0	2	0	4
21	Punjab	0	0	0	1	0	7	0	6
22	Rajasthan	0	0	0	0	0	0	0	42
23	Sikkim	0	0	0	0	0	0	0	50
									18
									18
									0
									0

(Continued)

Table 1.3 | (Continued)

Sr. No.	State/UT	Motives							Total
		Revenge/ Settling Scores	Greed/ Money	Extortion	Cause Disrepute	Prank/ Satisfaction of Gaining Control	Fraud/Illegal Gain	Eve Teasing/ Harassment	
24	Tamil Nadu	0	0	2	10	0	—	9	0
25	Tripura	0	0	0	0	0	0	0	0
26	Uttar Pradesh	0	1	0	0	1	0	2	4
27	Uttarakhand	0	0	0	0	0	0	0	0
28	West Bengal	0	0	0	0	0	0	0	0
	Total (States)	6	15	2	17	4	55	36	461
	<i>Union Territories</i>								
29	A & N Islands	0	0	0	0	0	0	0	0
30	Chandigarh	0	1	0	0	0	0	1	2
31	D & N Haveli	0	0	0	0	0	0	0	0
32	Daman & Diu	0	0	0	0	0	0	0	0
33	Delhi	0	0	0	0	2	1	15	18
34	Lakshadweep	0	0	0	0	0	0	0	0
35	Pondicherry	0	0	0	0	0	0	0	0
	Total (UTs)	0	1	0	0	2	1	16	20
	Total (All India)	6	16	2	17	4	57	37	481
	<i>Cities</i>								
36	Agra	0	0	0	0	0	1	0	1
37	Ahmedabad	0	2	0	1	0	0	5	9
38	Allahabad	0	0	0	0	0	0	0	0
39	Amritsar	0	0	0	0	0	0	0	0
40	Asansol	0	0	0	0	0	0	0	0
41	Bangalore	4	4	0	3	0	16	10	1
42	Bhopal	0	0	0	0	0	0	0	0
43	Chennai	0	0	2	10	0	8	0	20
44	Coimbatore	0	0	0	0	0	0	0	0

(Continued)

Table 1.3 | (Continued)

Sr. No.	State/UT	Motives							Total
		Revenge/ Settling Scores	Greed/ Money	Extortion	Cause Disrepute	Prank/ Satisfaction of Gaining Control	Fraud/Illegal Gain	Eve Teasing/ Harassment	
45	Delhi (City)	0	0	0	0	0	2	1	15
46	Dhanbad	0	0	0	0	0	0	0	0
47	Faridabad	0	0	0	0	0	0	3	3
48	Hyderabad	0	0	0	0	0	0	0	0
49	Indore	0	0	0	0	0	0	0	0
50	Jabalpur	0	0	0	0	0	0	0	0
51	Jaipur	0	0	0	0	0	0	0	0
52	Jamshedpur	0	0	0	0	0	0	0	0
53	Kanpur	0	0	0	0	0	0	0	0
54	Kochi	0	0	0	0	0	0	0	0
55	Kolkata	0	0	0	0	0	0	0	0
56	Lucknow	0	0	0	0	0	0	0	0
57	Ludhiana	0	0	0	0	0	0	0	0
58	Madurai	0	0	0	0	0	0	0	0
59	Meerut	0	0	0	0	0	0	0	0
60	Mumbai	0	5	0	0	0	0	1	2
61	Nagpur	0	0	0	0	0	1	2	0
62	Nasik	0	0	0	0	0	0	0	0
63	Patna	0	0	0	0	0	0	0	0
64	Pune	0	0	0	1	0	4	3	1
65	Rajkot	0	0	0	0	0	0	0	0
66	Surat	0	0	0	0	0	0	0	146
67	Vadodara	0	0	0	0	0	0	0	0
68	Varanasi	0	0	0	0	0	0	0	0
69	Vijayawada	0	0	0	0	0	2	0	2
70	Vishakhapatnam	0	0	0	0	0	0	0	0
Total (Cities)		4	11	2	15	0	26	173	257

Source: <http://nrcb.nic.in/crime2005/cii-2005/Table%2018.8.pdf> (1 March 2009).

Table 1.4 | 2005 Cases under cybercrime – part B

Sr. No.	State/UT	Suspects						Total
		Foreign National /Group	Disgruntled Employee/ Employees	Cracker/ Student/ Professional Learners	Business Competitor	Neighbors/ Friends and Relatives	Others	
States								
1	Andhra Pradesh	0	0	3	11	8	60	82
2	Arunachal Pradesh	0	0	0	0	0	0	0
3	Assam	0	0	0	0	0	1	1
4	Bihar	0	0	0	0	0	0	0
5	Chhattisgarh	0	0	20	0	0	26	46
6	Goa	0	0	0	0	0	3	3
7	Gujarat	0	2	2	1	0	150	155
8	Haryana	0	0	0	2	1	6	6
9	Himachal Pradesh	0	0	0	0	0	0	0
10	Jammu & Kashmir	0	0	0	0	0	0	0
11	Jharkhand	0	0	0	0	0	0	0
12	Karnataka	4	13	1	0	7	13	38
13	Kerala	0	0	0	0	0	0	0
14	Madhya Pradesh	0	0	0	0	0	0	0
15	Maharashtra	0	2	0	0	5	20	27
16	Manipur	0	0	0	0	0	0	0
17	Meghalaya	0	0	0	0	0	0	0
18	Mizoram	0	0	0	0	0	0	0
19	Nagaland	0	0	0	0	0	0	0
20	Orissa	0	0	0	2	0	4	6
21	Punjab	0	8	6	1	0	35	50
22	Rajasthan	0	0	11	0	0	7	18
23	Sikkim	0	0	0	0	0	0	0
24	Tamil Nadu	0	15	1	0	3	3	22
25	Tripura	0	0	0	0	0	0	0
26	Uttar Pradesh	0	0	2	0	0	2	4
27	Uttarakhand	0	0	0	0	0	0	0
28	West Bengal	0	0	0	0	0	0	0
Total (States)		4	40	46	17	24	330	458

(Continued)

Table 1.4 | (Continued)

Sr. No.	State/UT	Suspects						Total
		Foreign National /Group	Disgruntled Employee/ Employees	Cracker/ Student/ Professional Learners	Business Competitor	Neighbors/ Friends and Relatives	Others	
<i>Union Territories</i>								
29	A & N Islands	0	0	0	0	0	0	0
30	Chandigarh	0	0	1	0	0	1	2
31	D & N Haveli	0	0	0	0	0	0	0
32	Daman & Diu	0	0	0	0	0	0	0
33	Delhi	0	2	0	0	0	16	18
34	Lakshadweep	0	0	0	0	0	0	0
35	Pondicherry	0	0	0	0	0	0	0
	Total (UTs)	0	2	1	0	0	17	20
	Total (All India)	4	42	47	17	24	347	478
<i>Cities</i>								
36	Agra	0	0	0	0	0	1	1
37	Ahmedabad	0	2	2	1	0	4	9
38	Allahabad	0	0	0	0	0	0	0
39	Amritsar	0	0	0	0	0	0	0
40	Asansol	0	0	0	0	0	0	0
41	Bangalore	4	13	1	0	7	13	38
42	Bhopal	0	0	0	0	0	0	0
43	Chennai	0	14	0	0	3	3	20
44	Coimbatore	0	0	0	0	0	0	0
45	Delhi (City)	0	2	0	0	0	16	18
46	Dhanbad	0	0	0	0	0	0	0
47	Faridabad	0	0	0	0	0	3	3
48	Hyderabad	0	0	0	0	0	0	0
49	Indore	0	0	0	0	0	0	0
50	Jabalpur	0	0	0	0	0	0	0
51	Jaipur	0	0	0	0	0	0	0
52	Jamshedpur	0	0	0	0	0	0	0
53	Kanpur	0	0	0	0	0	0	0
54	Kochi	0	0	0	0	0	0	0
55	Kolkata	0	0	0	0	0	0	0
56	Lucknow	0	0	0	0	0	0	0
57	Ludhiana	0	0	0	0	0	0	0
58	Madurai	0	0	0	0	0	0	0
59	Meerut	0	0	0	0	0	0	0
60	Mumbai	0	0	0	0	0	8	8

(Continued)

Table 1.4 | (Continued)

Sr. No.	State/UT	Suspects						Total
		Foreign National /Group	Disgruntled Employee/ Employees	Cracker/ Student/ Professional Learners	Business Competitor	Neighbors/ Friends and Relatives	Others	
61	Nagpur	0	0	0	0	2	1	3
62	Nasik	0	0	0	0	0	0	0
63	Patna	0	0	0	0	0	0	0
64	Pune	0	0	0	0	1	8	9
65	Rajkot	0	0	0	0	0	0	0
66	Surat	0	0	0	0	0	146	146
67	Vadodara	0	0	0	0	0	0	0
68	Varanasi	0	0	0	0	0	0	0
69	Vijayawada	0	0	0	2	0	0	2
70	Vishakhapatnam	0	0	0	0	0	0	0
Total (Cities)		4	31	3	3	13	203	257

Source: <http://ncrb.nic.in/crime2005/cii-2005/Table%2018.8.pdf> (1 March 2009).

- 2. Techno-vandalism:** These acts of “brainless” defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards, should prevent the vast majority of such incidents.

There is a very thin line between the two terms “computer crime” and “computer fraud”; both are punishable (see Tables 1.1–1.4). Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways: (a) how to commit them is easier to learn, (b) they require few resources relative to the potential damage caused, (c) they can be committed in a jurisdiction without being physically present in it and (d) they are often not clearly illegal.

The term cybercrime has some stigma attached and is notorious due to the word “terrorism” or “terrorist” attached with it, that is, cyberterrorism (see explanation of the term in Box 1.1). Cyberterrorism is defined as “any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism.” Cybercrime, especially through the Internet, has grown in number as the use of computer has become central to commerce, entertainment and government.

The term *cyber* has some interesting synonyms: fake, replicated, pretend, imitation, virtual, computer-generated. Cyber means combining forms relating to Information Technology, the Internet and Virtual Reality. This term owes its origin to the word “cybernetics” which deals with information and its use; furthermore, cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation.^[2] However, beyond this, there does not seem to be any further connection to the term “cybernetics” as per other sources searched.^[3–5] According to Wikipedia,^[6] cybernetics is the interdisciplinary study of the structure of regulatory systems. It is closely related to control theory and systems theory.

People are curious to know how cybercrimes are planned and how they actually take place (explained in Chapter 2). Worldwide, including India, cyberterrorists usually use computer as a tool, target or both for

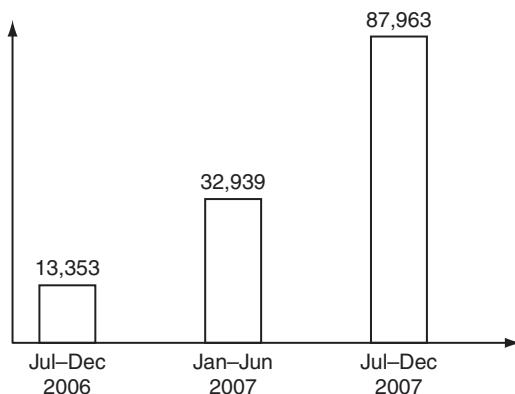


Figure 1.2 | Rise in the number of Phishing hosts.

Source: Symantec (International Telecommunications Society, 17th Biennial Conference, Montreal, Canada, June 24–27, 2008).

their unlawful act to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information. [See Further Reading, Books, Ref. #3 for a pointer to data privacy and understanding terms such as sensitive information, personal information (PI) and sensitive personal information (SPI).] Internet is one of the means by which the offenders can gain priced sensitive information of companies, firms, individuals, banks and can lead to intellectual property (IP) crimes (such as stealing new product plans, its description, market program plans, list of customers, etc.), selling illegal articles, pornography/child pornography, etc. This is done using methods such as Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual. “Phishing” refers to an attack using mail programs to deceive or coax Internet users into disclosing confidential information that can be then exploited for illegal purposes. Figure 1.2 shows the increase in Phishing hosts.

1.3 Cybercrime and Information Security

Lack of information security gives rise to cybercrimes. This subject is explained in greater detail in Chapter 9. Let us refer to the amended Indian Information Technology Act (ITA) 2000^[7] in the context of cybercrime. From an Indian perspective, the new version of the Act (referred to as *ITA 2008*) provides a new focus on “Information Security in India.” “Cybersecurity” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. The term incorporates both the physical security of devices as well as the information stored therein. It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction. (For a thorough discussion about these aspects, see Ref. #2, Books, Further Reading.)

Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft. The 2008 CSI Survey^[8] on computer crime and security supports this. Cybercrimes occupy an important space in information security domain because of their impact. For anyone trying to compile data on business impact of cybercrime, there are number of challenges. One of them comes from the fact that organizations do not explicitly incorporate the cost of the vast majority of computer security incidents into their accounting as opposed to, say,

Box 1.2 The Botnet Menace!

The topic of Botnets is discussed in Section 2.6, Chapter 2. The term "Botnet" is used to refer to a group of compromised computers (zombie computers, i.e., personal computers secretly under the control of hackers) running malwares under a common command and control infrastructure. Figure 1.3 shows how a "zombie" works.

A Botnet maker can control the group remotely for illegal purposes, the most common being denial-of-service attack (DoS attack), Adware, Spyware, E-Mail Spam, Click Fraud (see reference links provided in Ref. #5, Articles and Research Papers, Further Reading), theft of application serial numbers, login IDs and financial information such as credit card numbers, etc. An attacker usually gains control by infecting the computers with a virus or other Malicious Code. The computer may continue to operate normally without the owner's knowledge that his computer has been compromised. The topic of computer viruses is addressed in Chapter 4 (Section 4.6).

The problem of Botnet is global in nature and India is also facing the same. India has an average of 374 new Bot attacks per day and had more than 38,000 distinct Bot-infected computers in the first half of the year 2009. Small and medium businesses in the country are at greater risk, as they are highly vulnerable to Bots, Phishing, Spam and Malicious Code attacks. Mumbai with 33% incidences tops the Bot-infected city list, followed by New Delhi at 25%, Chennai at 17% and Bangalore at 13%. Tier-II locations are now also a target of Bot-networks with Bhopal at 4% and Hyderabad, Surat, Pune and Noida at 1% each.

The Internet is a network of interconnected computers. If the computers, computer systems, computer resources, etc. are unsecured and vulnerable to security threats, it can be detrimental to the critical infrastructure of the country. We have witnessed the incidence of Cyberwar against Estonia and the same is possible against any country including India.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India (Chapter 3, Section 3.7, Fig. 3.8).

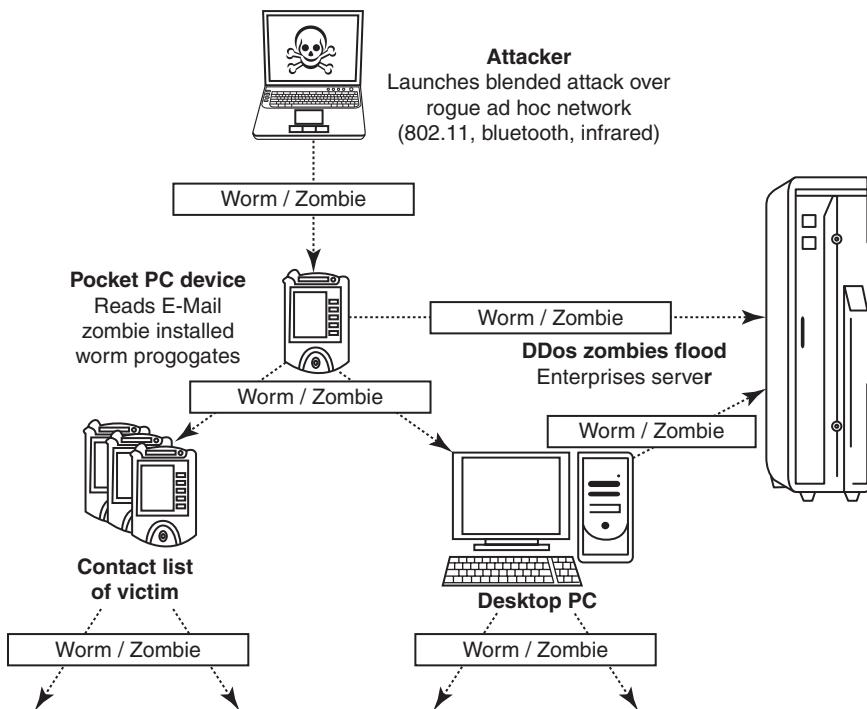


Figure 1.3 | How a zombie works.

accounting for the “shrinkage” of goods from retail stores. The other challenge comes from the difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost (most notably through loss/theft of laptops, see the survey conducted by Ponemon Institute in Ref. #19, Additional Useful Web References, Further Reading). Because of these reasons, reporting of financial losses often remains approximate. In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about “security incidents” including cybercrime. In general, organizations perception about “insider attacks” seems to be different than that made out by security solution vendor. However, this perception of an organization does not seem to be true as revealed by the 2008 CSI Survey. Awareness about “data privacy” too tends to be low in most organizations. When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such “crimes” may not be detected by the victimized organization and no direct costs may be associated with the theft (Table 1.5).

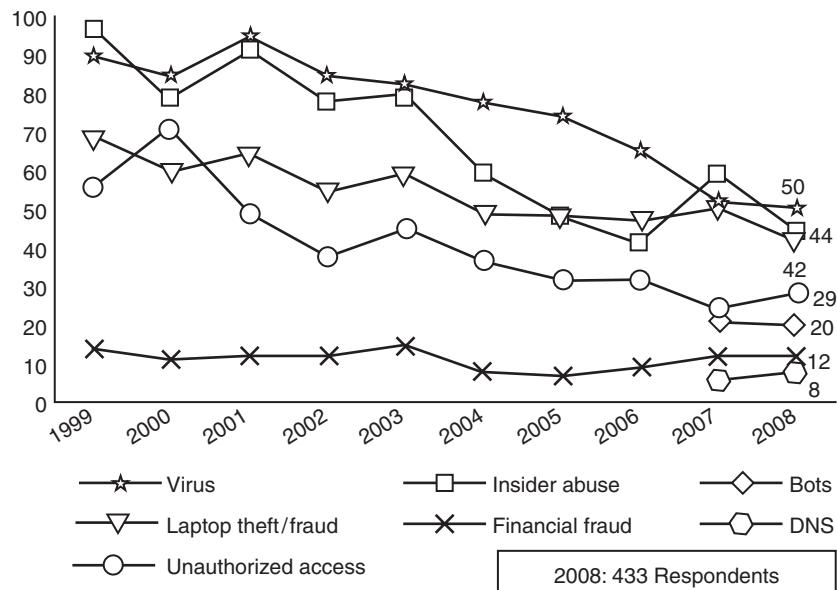
Figure 1.4 shows several categories of incidences – *viruses*, *insider abuse*, *laptop theft* and *unauthorized access* to systems. Refer to Ref. #1 (Chapter 3, Section 3.11), Book, Further Reading for laptop threats and information security implications in mobile computing paradigm and “thefts/losses.” Also read Chapter 9 of this book.

Typical network misuses are for Internet radio/streaming audio, streaming video, file sharing, instant messaging and online gaming (such as online poker, online casinos, online betting, etc.; refer to <http://>

Table 1.5 | Cybercrime trend over the years (1999–2008)

<i>Types of Cybercrime</i>	<i>2004 (%)</i>	<i>2005 (%)</i>	<i>2006 (%)</i>	<i>2007 (%)</i>	<i>2008 (%)</i>
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11
Bots (see Box 1.2; more in Chapter 2)				21	20
DoS attacks				6	8
Instant messaging abuse				25	21
Password sniffing (explained in Chapter 2)				10	9
Theft/loss of customer data				17	17
• from mobile devices					8
• from all other sources					8

Source: 2008 CSI Computer Crime and Security Survey available at the link <http://i.cmpnet.com/v2.goci.com/pdf/CSIsurvey2008.pdf> (15 March 2009).

**Figure 1.4** Major types of incidents by percentage.

Source: 2008 CSI Computer Crime and Security Survey available at the link <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf> (15 March 2009).

en.wikipedia.org/wiki/Online_gambling). Online gambling is illegal in some countries – for example, in India. However, India has yet to pass laws that specifically deal with the issue, leaving a sort of legal loophole in the meantime. (In Ref. #20, Additional Useful Web References, Further Reading, we have provided links to refer to about legal status of online gambling in India. The Indian online gambling market is estimated to be worth 1–5 billion US\$!).

1.4 Who are Cybercriminals?

Cybercrime involves such activities as child pornography; credit card fraud; cyberstalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark protection; overriding encryption to make illegal copies; software piracy and stealing another's identity (known as identity theft) to perform criminal acts (see detailed discussion on identity theft in Chapter 5). Cybercriminals are those who conduct such acts. They can be categorized into three groups that reflect their motivation (see Ref. #2, Books, Further Reading):

1. **Type I: Cybercriminals – hungry for recognition**
 - Hobby hackers;
 - IT professionals (social engineering is one of the biggest threat);
 - politically motivated hackers;
 - terrorist organizations.
2. **Type II: Cybercriminals – not interested in recognition**
 - Psychological perverts;
 - financially motivated hackers (corporate espionage);

- state-sponsored hacking (national espionage, sabotage);
- organized criminals.

3. Type III: Cybercriminals – the insiders

- Disgruntled or former employees seeking revenge;
- competing companies using employees to gain economic advantage through damage and/or theft.

Thus, the typical “motives” behind cybercrime seem to be greed, desire to gain power and/or publicity, desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mindset and desire to sell network security services. This is explained in Chapter 10. Cybercafes are known to play role in committing cybercrimes. A link about cybercafes under ITA 2008 (amendment to Indian ITA 2000) is provided in Ref. #23, Additional Useful Web References, Further Reading. Another link, describing views if the amended ITA 2000 is stringent enough for cybercriminals, is provided in the same section as Ref. #24.

1.5 Classifications of Cybercrimes

Table 1.6 presents a scheme for cybercrime classification (broad and narrow classification).

Crime is defined as “*an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law*” (Webster Dictionary). Cybercrimes are classified as follows:

1. Cybercrime against individual

- *Electronic mail (E-Mail) Spoofing and other online frauds*: Refer to Section 1.5.1 of this chapter and Chapter 4 for more details.
- *Phishing, Spear Phishing* and its various other forms such as Vishing (Section 3.8.4) and Smishing (Section 3.8.5): Refer to Chapter 5 for discussion about Phishing and Spear Phishing.
- *Spamming*: It is explained in Section 1.5.2.
- *Cyberdefamation*: It is explained later in Section 1.5.3.
- *Cyberstalking and harassment*: It is explained in Chapter 2.
- *Computer sabotage*: It is explained later in Section 1.5.15.
- *Pornographic offenses*: It is explained in Section 1.5.13.
- *Password sniffing*: This also belongs to the category of cybercrimes against organization because the use of password could be by an individual for his/her personal work or the work he/she is doing using a computer that belongs to an organization. It is explained in Section 1.5.19 (also see Table 1.5).

Table 1.6 | Classifying cybercrimes – broad and narrow

	<i>Cybercrime in Narrow Sense</i>	<i>Cybercrime in Broad Sense</i>	
Role of computer	<i>Computer as an object</i> The computer/information stored on the computer is the subject/target of the crime	<i>Computer as a tool</i> The computer/or information stored on the computer constitutes an important tool for committing the crime	<i>Computer as the environment or context</i> The computer/information stored on the computer plays a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, computer sabotage, DDoS-attacks (distributed denial-of-service attacks), virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

2. Cybercrime against property

- *Credit card frauds:* Refer to Chapter 5 for Phishing and Spear Phishing and Chapter 11, Section 11.4 (in CD).
- *Intellectual property (IP) crimes:* Basically, IP crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code, etc. (refer to Chapters 9 and 10).
- *Internet time theft:* It is explained in Section 1.5.4 as well as in Chapter 11 (Mini-Case 4, Section 11.3.4).

3. Cybercrime against organization

- *Unauthorized accessing of computer:* Hacking is one method of doing this and hacking is a punishable offense (see point 2 in Box 1.7).
- *Password sniffing:* It is explained in Section 1.5.19 (also see Table 1.5).
- *Denial-of-service attacks* (known as DoS attacks): It is explained more in detail in Chapter 4.
- *Virus attack/dissemination of viruses:* Refer to Chapter 4 for detailed discussion on this.
- *E-Mail bombing/mail bombs:* It is explained in Section 1.5.16.
- *Salami attack/Salami technique:* It is explained in Section 1.5.5.
- *Logic bomb:* It is explained in Section 1.5.15 (Computer Sabotage).
- *Trojan Horse:* It is explained more in detail in Chapter 4.
- *Data diddling:* It is explained in Section 1.5.6. Refer to Section 11.2.6, Chapter 11.
- *Crimes emanating from Usenet newsgroup:* It is explained in Section 1.5.9.
- *Industrial spying/industrial espionage:* It is explained in Section 1.5.10.
- *Computer network intrusions:* It is explained in Section 1.5.18.
- *Software piracy –* It is explained in Section 1.5.14. Also refer to Section 9.2.2, Chapter 9.

4. Cybercrime against Society

- *Forgery:* It is explained in Section 1.5.7 (see Table 1.6 and Box 1.6).
- *Cyberterrorism:* Refer to Box 1.1 and Box 1.7, and Section 1.2 for detailed discussion on this.
- *Web jacking:* It is explained in Section 1.5.8.

5. Crimes emanating from Usenet newsgroup:

By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.

Let us take a brief look at some of the cybercrime forms mentioned above.

1.5.1 E-Mail Spoofing

A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source. For example, let us say, Roopa has an E-Mail address roopa@asianlaws.org. Let us say her boyfriend Suresh and she happen to have a show down. Then Suresh, having become her enemy, spoofs her E-Mail and sends obscene/vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa, her friends could take offense and relationships could be spoiled for life. See Box 2.7 in Chapter 2.

1.5.2 Spamming

People who create electronic Spam are called *spammers*. Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media: instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions, social networking Spam, file sharing network Spam, video sharing sites, etc.

Spamming is difficult to control because it has economic viability – advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Spammers are numerous; the volume of unsolicited mail has become very high because the barrier to entry is low. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers (ISPs), who are forced to add extra capacity to cope with the deluge. Spamming is widely detested, and has been the subject of legislation in many jurisdictions – for example, the CAN-SPAM Act of 2003.

Another definition of spamming is in the context of “search engine spamming.” In this context, spamming is alteration or creation of a document with the intent to deceive an electronic catalog or a filing system. Some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned search results – this is strongly discouraged by search engines and there are fines/penalties associated with the use of such subversive techniques. Those who continually attempt to subvert or Spam the search engines may be permanently excluded from the search index. Therefore, the following web publishing techniques should be avoided:

1. Repeating keywords;
2. use of keywords that do not relate to the content on the site;
3. use of fast meta refresh;
4. redirection;
5. IP Cloaking;
6. use of colored text on the same color background;
7. tiny text usage;
8. duplication of pages with different URLs;
9. hidden links;
10. use of different pages that bridge to the same URL (gateway pages).

Further discussion on each of the above is beyond the scope of this chapter which is meant to be only an overview of cybercrimes.

1.5.3 Cyberdefamation



Cyberdefamation is a cognizable offense.

Let us first understand what the term entails. CHAPTER XXI of the Indian Penal Code (IPC) is about DEFAMATION. In Section 499 of CHAPTER XXI of IPC, regarding “defamation” there is a mention that

“Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.”

Cyberdefamation happens when the above takes place in an electronic form. In other words, “cyberdefamation” occurs when defamation takes place with the help of computers and/or the Internet, for example, someone publishes defamatory matter about someone on a website or sends an E-Mail containing defamatory information to all friends of that person. According to the IPC Section 499:

1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Box 1.3 \ Internet: A New Fuel for Defamation?

The Web allows an instant global publication of information at a very low cost. Information, which would not normally be revealed prior to the advent of the Internet, can now be obtained by practically anyone. The relatively low cost of connecting to the Internet and the ease of establishing one's own website means that the opportunity for defamation has increased considerably. Now, on the Internet everyone may be a publisher and may be sued as a publisher. A key feature of the Internet is that users do not have to reveal their true identity to send E-Mail or post messages on bulletin boards. Figure 1.5 shows the humor regarding this on the lighter side. Users are able to communicate and make such postings anonymously or under assumed names.

"Faceless" communication channel is the unique feature brought about by the Internet. Not only that but also people can access the Internet in privacy and seclusion of their own homes or offices. These features of the Internet plus the interactive, responsive nature of communications on the Internet means that now the users are far less inhibited about the contents of their messages resulting in cyberspace becoming excessively prone to defamation.

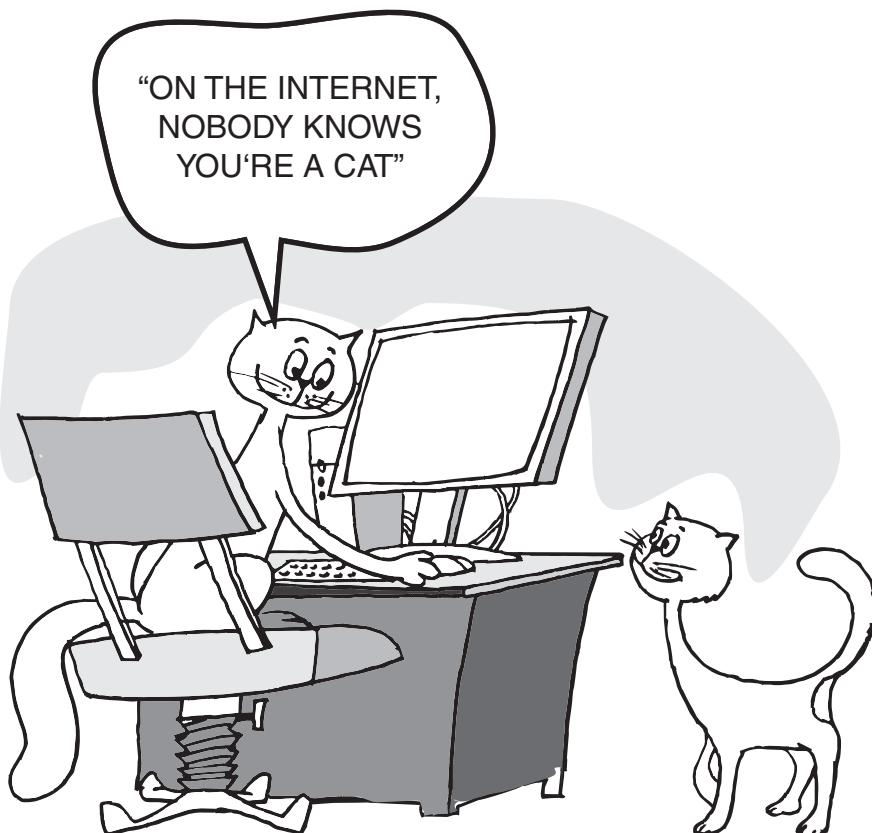


Figure 1.5 | Anonymity for Internet users.

2. It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.
3. An imputation in the form of an alternative or expressed ironically, may amount to defamation.
4. No imputation is said to harm a person's reputation unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state or in a state generally considered as disgraceful.

Libel is written defamation and *slander* is oral defamation. When determining whether or not defamation has taken place, the only issue to consider is whether a person of ordinary intelligence in society would believe that the words would indeed injure the person's reputation. Even if there is no (apparent) damage to a person's reputation, the person who made the allegations may still be held responsible for defamation.

The law on defamation attempts to create a workable balance between two equally important human rights: *The right to an unimpaired reputation* and *the right to freedom of expression*. In a cybersociety, both these interests are increasingly important. Protection of reputation is arguably even more important in a highly technological society, because one may not even encounter an individual or organization other than through the medium of the Internet. Some courts have held that the plaintiff must also have to show that the defamatory statements were unlawful and that it must not be for the defendant to justify his conduct by showing that the statements were in accordance with law. India's first case of cyberdefamation, at the Delhi Court, assumed jurisdiction over a matter where a corporate reputation was being defamed through E-Mails and passed an important ex-parte injunction. Further details on this case can be read at the link <http://cyberlaws.net/cyberindia/defamation.htm> (14 December 2009). Readers can also refer to the link http://en.wikipedia.org/wiki/Cyber_defamation_law (14 December 2009) for understanding cyberdefamation law.

1.5.4 Internet Time Theft

Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person. Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent. The issue of Internet time theft is related to the crimes conducted through "identity theft." In Chapter 11, there is a case described about theft of Internet time.

1.5.5 Salami Attack/Salami Technique

These attacks are used for committing financial crimes. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed; for example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say ₹ 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month. In Chapter 11, there are a number of examples, illustrations provided about use of Salami Technique in real life. Refer to Section 11.2 Real-Life Examples (Section 11.2.13 Example 13: Small "Shavings" for Big Gains! and Section 11.2.20 Example 20: The Petrol Pump Fraud).

1.5.6 Data Diddling

A data diddling attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling

programs inserted when private parties computerize their systems. In Chapter 11, there are a number of data diddling examples (refer to Section 11.2.6 Example 6: Doodle me Diddle!).

1.5.7 Forgery

Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake marksheets or even degree certificates. These are made using computers and high quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

1.5.8 Web Jacking

Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves “password sniffing.” The actual owner of the website does not have any more control over what appears on that website.

1.5.9 Newsgroup Spam/Crimes Emanating from Usenet Newsgroup

As explained earlier, this is one form of spamming. The word “Spam” was usually taken to mean excessive multiple posting (EMP). The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever. Spaming of Usenet newsgroups actually predates E-Mail Spam. The first widely recognized Usenet Spam titled *Global Alert for All: Jesus is Coming Soon* (though not the most famous) was posted on 18 January 1994 by Clarence L. Thomas IV, a sysadmin at Andrews University. It was a fundamentalist religious tract claiming that “this world’s history is coming to a climax.” The newsgroup posting Bot Serdar Argic also appeared in early 1994, posting tens of thousands of messages to various newsgroups, consisting of identical copies of a political screed relating to the Armenian Genocide.

1.5.10 Industrial Spying/Industrial Espionage

Spying is not limited to governments. Corporations, like governments, often spy on the enemy. The Internet and privately networked systems provide new and better opportunities for espionage. “Spies” can get information about product finances, research and development and marketing strategies, an activity known as “industrial spying.” However, cyberspies rarely leave behind a trail. Industrial spying is not new; in fact it is as old as industries themselves. The use of the Internet to achieve this is probably as old as the Internet itself. Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of escrow organizations (it is said that they get several hundreds of thousands of dollars, depending on the “assignment”).

With the growing public availability of Trojans and Spyware material (for Trojans and Spyware discussion, refer to Chapter 4 in the book and Chapter 3 of Ref. #1, Books, Further Reading), even low-skilled individuals are now inclined to generate high volume profit out of industrial spying. This is referred to as “Targeted Attacks” (which includes “Spear Phishing”). This aspect of *Industrial Spying* is the one to be addressed in the fight against cybercrime.

Organizations subject to online extortion tend to keep quiet about it to avoid negative publicity about them. Not surprisingly, this also applies very well to organizations that are victim of focused attacks aiming at stealing corporate data, Intellectual Property or whatever else that may yield a competitive advantage for a rival company.

One interesting case is the famous Israeli Trojan story,^[9] where a software engineer in London created a Trojan Horse program specifically designed to extract critical data gathered from machines infected by his program. He had made a business out of selling his Trojan Horse program to companies in Israel, which would use it for industrial spying by planting it into competitors' networks. The methods used to inoculate the Trojan Horse were varied and sometimes quite inventive, ranging from simple E-Mail traps to the mailing of promotional CDs infected with the evil program! More about Trojan Horse is addressed in Chapter 2.

There are also the E-Mail worms automating similar "data exfiltration features." For example, the main characteristic of mass mailing worm deemed W32.Myfp.A^[10] is to scan the hard drive of infected machines for all files with the following extensions: .pdf, .doc, .dwg, .sch, .pcb, .dwt, .dwf, .max, .mdb. Such files are uploaded on an FTP server owned by the cybercrooks, with the aim of stealing as much IP as possible wherever it can be and then selling it to people who are ready to pay for it. There are two distinct business models for cybercrime applied to industrial spying: *Selling Trojan-ware* and *Selling Stolen Intellectual Property*.

1.5.11 Hacking

Although the purposes of hacking are many, the main ones are as follows:

1. Greed;
2. power;
3. publicity;
4. revenge;
5. adventure;
6. desire to access forbidden information;
7. destructive mindset.

Every act committed toward breaking into a computer and/or network is hacking and it is an offense. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information that is critical in nature. Government websites are hot on hackers' target lists and attacks on Government websites receive wide press coverage. For example, according to the story posted on December 2009, the NASA site was hacked via SQL Injection (see Ref. #22, Additional Useful Web References, Further Reading). SQL Injection is covered more in detail in Chapter 4. Examples of prominent websites hacked are shown in Figs. 1.6–1.10.

Hackers, crackers and phrackers^[11] are some of the oft-heard terms. The original meaning of the word "hack" meaning an elegant, witty or inspired way of doing almost anything originated at MIT. The meaning has now changed to become something associated with the breaking into or harming of any kind of computer or telecommunications system. Some people claim that those who break into computer systems should ideally be called "crackers" and those targeting phones should be known as "phreaks" (see Chapter 17, Box 17.3 of Ref. #3, Books, Further Reading).

1.5.12 Online Frauds

Refer to Chapter 11, Section 11.7: Online Scams. There are a few major types of crimes under the category of hacking: Spoofing website and E-Mail security alerts, hoax mails about virus threats (refer to Chapter 4), lottery frauds and Spoofing. In Spoofing websites and E-Mail security threats, fraudsters create authentic

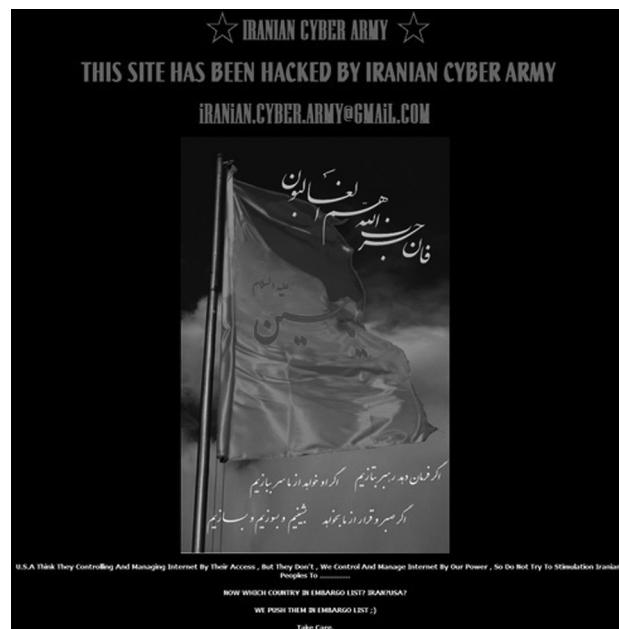


Figure 1.6 Twitter site hacked.

Source: <http://thenextweb.com/files/2009/12/Twitter-Hacked.png/> (14 July 2010).

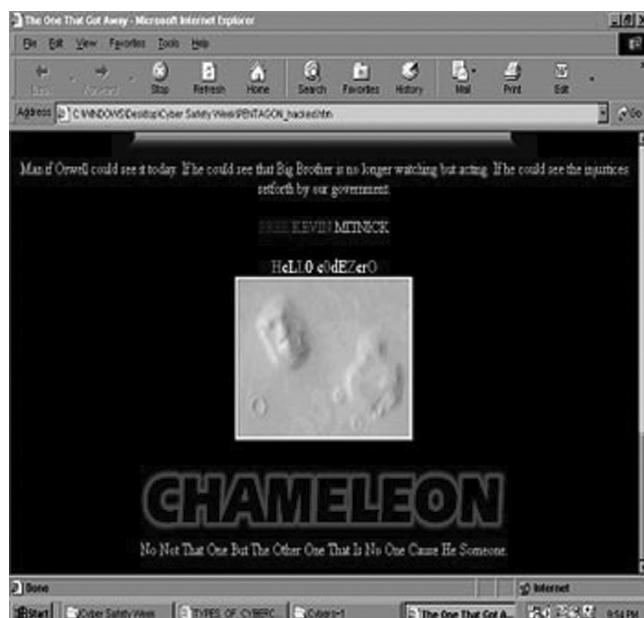


Figure 1.7 Pentagon, the US site defaced.

Source: <http://www.keylogger.org/news-world/hackers-attack-pentagon-1086.html>

Box 1.4 The Story of a Hacked Website

Nadya Suleman (Nadya Denise Doud-Suleman Gutierrez), famously known as "Octomom" in the media, is an American woman who came to international attention when she gave birth to octuplets in January 2009. Nadya launched a website to solicit donations for her family. However, her site was immediately hacked by a group of vigilante mothers! Nadya's website originally featured photos of all eight octuplets, a thank you note from Suleman, images of children's toys and a large donation button for viewers to send money through. Suleman also provided an address where people can send items such as diapers and baby food formula. The site was hacked and brought down within hours. The original homepage was left defaced as seen in Fig. 1.8.

The site was tagged by the famous hacker group MOD, also known as the Mothers of Disappointment. The mysterious group has a history of attacking personal sites they disapprove of; so much for the "psychology" of hackers! Probably these "Mothers" were hungry for "recognition" (recall the classification of cybercriminals in Section 1.4).

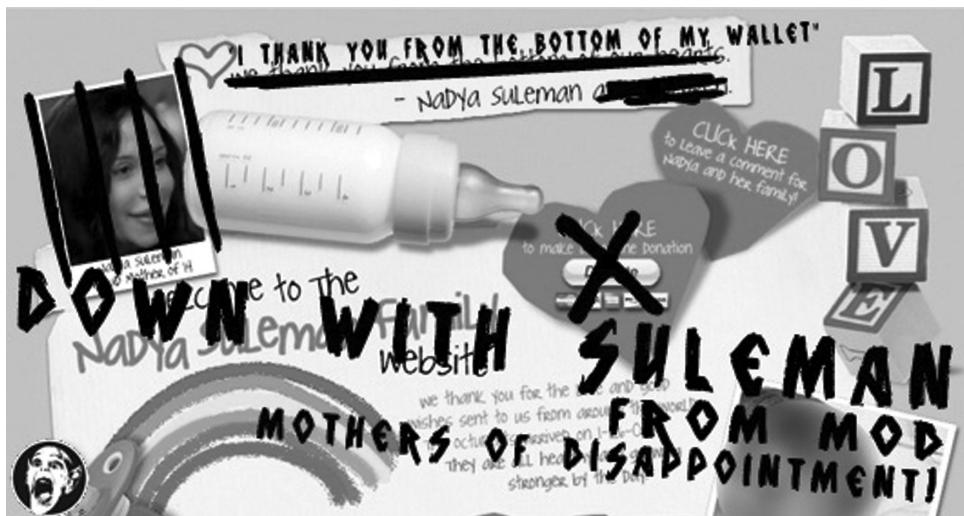


Figure 1.8 | Octomom's defaced website.

Source: <http://weeklyworldnews.com/headlines/6233/nadya-sulemans-website-hacked/>

looking websites that are actually nothing but a spoof (see Chapter 5 for details of Spoofing). The purpose of these websites is to make the user enter personal information which is then used to access business and bank accounts. Fraudsters are increasingly turning to E-Mail to generate traffic to these websites. This kind of online fraud is common in banking and financial sector. Refer to Chapter 11, Section 11.4. There is a rise in the number of financial institutions' customers who receive such E-Mails which usually contain a link to a spoof website and mislead users to enter user ids and passwords on the pretence that security details can be updated or passwords changed. It is wise to be alert and careful about E-Mails containing an embedded link, with a request for you to enter secret details. It is strongly recommended not to input any sensitive information that might help criminals to gain access to sensitive information, such as bank account details, even if the page appears legitimate.

In virus hoax E-Mails, the warnings may be genuine, so there is always a dilemma whether to take them lightly or seriously. A wise action is to first confirm by visiting an antivirus site such as McAfee, Sophos or Symantec before taking any action, such as forwarding them to friends and colleagues.

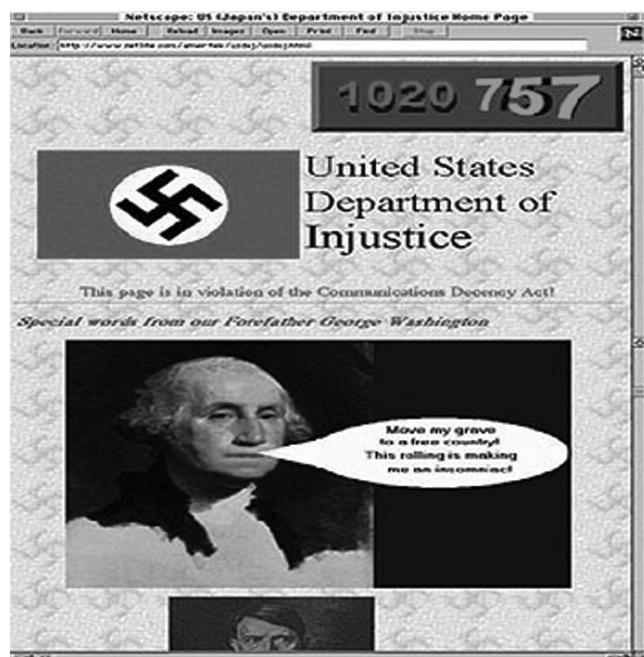


Figure 1.9 | Department of justice site defaced.

Source: <http://www.technize.com/see-all-the-hacked-and-defaced-websites/>

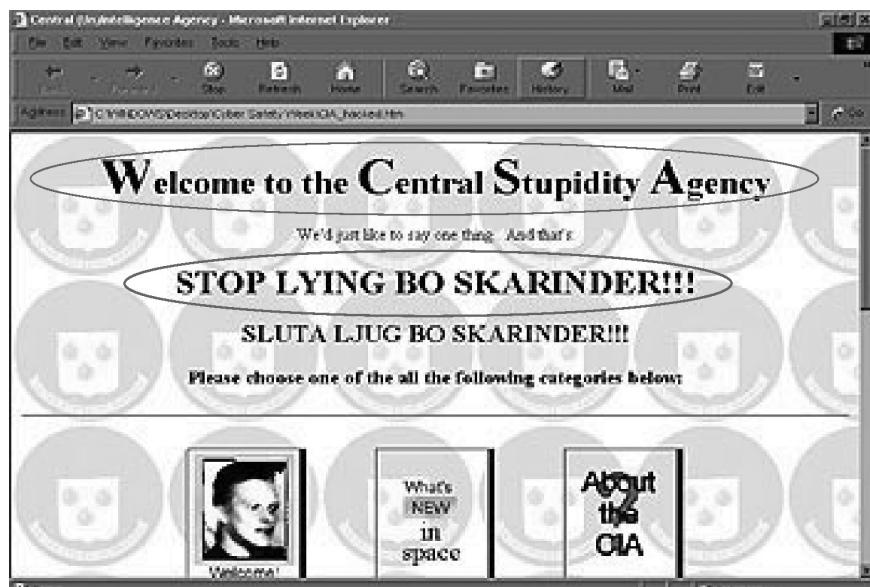


Figure 1.10 | CIA (Central Intelligence Agency), the US, website defaced.

Source: <http://www.technize.com/see-all-the-hacked-and-defaced-websites/>

Lottery frauds are typically letters or E-Mails that inform the recipient that he/she has won a prize in a lottery. To get the money, the recipient has to reply, after which another mail is received asking for bank details so that the money can be directly transferred. The E-Mail also asks for a processing fee/handling fee. Of course, the money is never transferred in this case; the processing fee is swindled and the banking details are used for other frauds and scams. Refer to Section 11.7.6, Chapter 11.

“Spoofing” means illegal intrusion, posing as a genuine user. A hacker logs-in to a computer illegally, using a different identity than his own. He is able to do this by having previously obtained the actual password. He creates a new identity by fooling the computer into thinking that the hacker is the genuine system operator and then hacker then takes control of the system. He can commit innumerable number of frauds using this false identity.

1.5.13 Pornographic Offenses

“Child pornography” means any visual depiction, including but not limited to the following:

1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
2. film, video, picture;
3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

Child pornography is considered an offense. Unfortunately, child pornography is a reality of the Internet. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. In India too, the Internet has become a household commodity in the urban areas of the nation. Its explosion has made the children a viable victim to the cybercrime. As the broad-band connections get into the reach of more and more homes, larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles. “Pedophiles” are people who physically or psychologically coerce minors to engage in sexual activities, which the minors would not consciously consent to. Here is how pedophiles operate:

- Step 1:** Pedophiles use a false identity to trap the children/teenagers (using “false identity” which in itself is another crime called “identity theft”). ID Theft is addressed in Chapter 5.
- Step 2:** They seek children/teens in the kids’ areas on the services, such as the Teens BB, Games BB or chat areas where the children gather.
- Step 3:** They befriend children/teens.
- Step 4:** They extract personal information from the child/teen by winning his/her confidence.
- Step 5:** Pedophiles get E-Mail address of the child/teen and start making contacts on the victim’s E-Mail address as well. Sometimes, these E-Mails contain sexually explicit language.
- Step 6:** They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
- Step 7:** At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

This is the irony of the “digital world”; in physical world, parents know the face of dangers and they know how to avoid and face the problems by following simple rules and accordingly they advise their children to keep away from dangerous things and ways. However, it is possible, even in the modern times most parents may not know the basics of the Internet and the associated (hidden) dangers from the services offered over

the Internet. Hence most children may remain unprotected in the cyberworld. Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is right/wrong for them while browsing the Internet. Legal remedies exist only to some extent; for example, Children's Online Privacy Protection Act or COPPA is a way of preventing online pornography. Interested readers are referred to COPPA sites.^[12] Readers would like to note that Net Nanny and Cybersitter^[13] are software, originally designed for parents concerned about their children's unrestricted access to the seamier side of the Internet, which can be used to block a user's access to websites containing "dangerous" or "offensive" material.

1.5.14 Software Piracy

This is a big challenge area indeed. (Readers may like to refer to Chapter 38 and other relevant pages of Ref. #3, Books, Further Reading.) Cybercrime investigation cell of India defines "software piracy" as *theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original*. There are many examples of software piracy: *end-user copying* – friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses; *hard disk loading with illicit means* – hard disk vendors load pirated software; *counterfeiting* – large-scale duplication and distribution of illegally copied software; *illegal downloads from the Internet* – by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose: (a) getting untested software that may have been copied thousands of times over, (b) the software, if pirated, may potentially contain hard-drive-infecting viruses, (c) there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users, (d) there is no warranty protection, (e) there is no legal right to use the product, etc.

Economic impact of software piracy is grave (see Fig. 1.11). According to the Fourth Annual BSA and IDC Global Software Piracy Study,^[14] in Asia Pacific 55% of the software installed in 2006 on personal computers (PCs) was obtained illegally, while software losses due to software piracy amounted to US\$ 11.6 billion. The Global Software Piracy Study mentioned covers all packaged software that runs on personal computers, including desktops, laptops and ultraportables. The study includes operating systems, systems software such as databases and security packages, business applications and consumer applications such as PC games, personal finance and reference software. Refer to Section 9.2.2, Chapter 9.

The BSA/IDC study of year 2006 did not include other types of software such as those which run on servers or mainframes or software sold as a service. It is shocking to know that 35% of the software installed in 2006 on PCs worldwide was obtained illegally, amounting to nearly \$40 billion in global losses due to software piracy. Progress was seen in a number of emerging markets, most notably in China, where the piracy rate dropped 10 percentage points in 3 years, and in Russia, where piracy fell seven percentage points over 3 years. Figure 1.12 shows the regional scenario on piracy rate.

1.5.15 Computer Sabotage

The term "sabotage" has been mentioned many times in this chapter (Table 1.5, Section 1.2, Section 1.4 – Type II criminals, Table 1.6). The use of the Internet to hinder the normal functioning of a computer system through the introduction of worms, viruses (refer to Chapter 4) or logic bombs, is referred to as computer sabotage. It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes. Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs. Some viruses may be termed as logic bombs because they lie dormant all through the

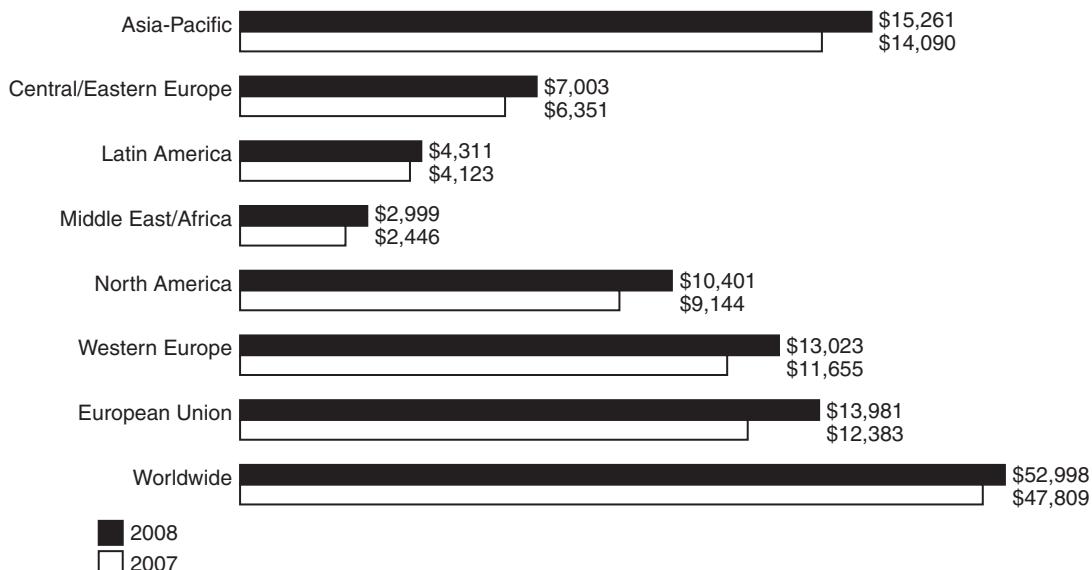


Figure 1.11 Dollars lost (year 2008) due to (software) piracy – regional scenario.

Source: BSA-IDC Global 2008 Piracy Study released on May 2009 at the following link:
<http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf> (29 January 2010).

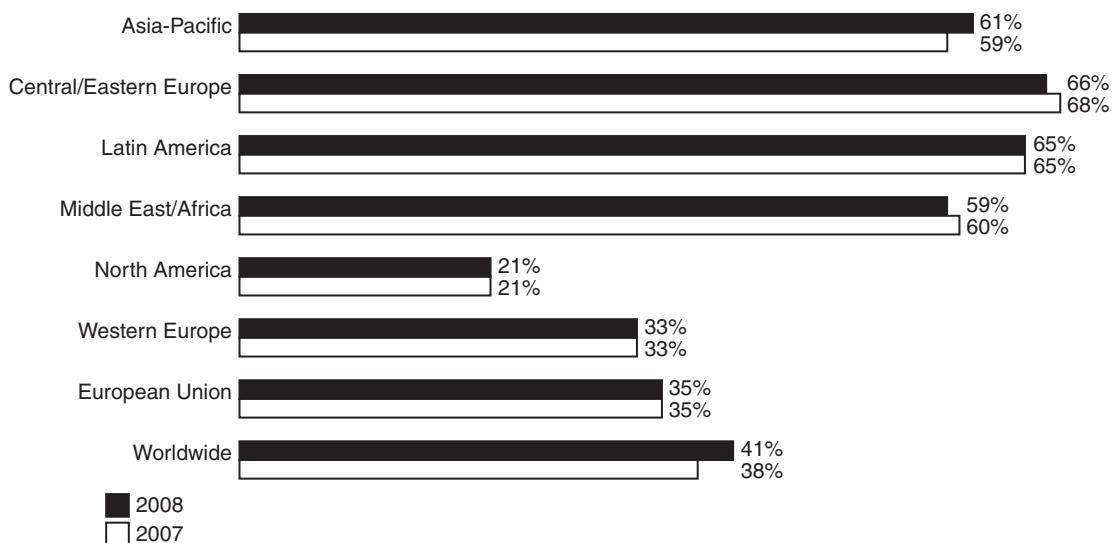


Figure 1.12 Regional picture on piracy rate.

Source: BSA-IDC Global 2008 Piracy Study released on May 2009 at the following link:
<http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf> (29 January 2010).

year and become active only on a particular date (e.g., the Chernobyl virus and Y2K viruses^[15]). Next, let us understand the term “mail bombs.”

1.5.16 E-Mail Bombing/Mail Bombs

E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim’s E-Mail account (in the case of an individual) or to make victim’s mail servers crash (in the case of a company or an E-Mail service provider). Computer program can be written to instruct a computer to do such tasks on a repeated basis. In recent times, terrorism has hit the Internet in the form of mail bombings. By instructing a computer to repeatedly send E-Mail to a specified person’s E-Mail address, the cybercriminal can overwhelm the recipient’s personal account and potentially shut down entire systems. This may or may not be illegal, but it is certainly disruptive. Refer to Box 1.2, Tables 1.5 and 1.6 and Chapter 4 for DoS attacks.

1.5.17 Usenet Newsgroup as the Source of Cybercrimes

Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects. Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics. In principle, it is possible to prevent the distribution of specific newsgroup. In reality, however, there is no technical method available for controlling the contents of any newsgroup. It is merely subject to self-regulation and net etiquette. It is feasible to block specific newsgroups, however, this cannot be considered as a definitive solution to illegal or harmful content. It is possible to put Usenet to following criminal use:

1. Distribution/sale of pornographic material;
2. distribution/sale of pirated software packages;
3. distribution of hacking software;
4. sale of stolen credit card numbers. Refer to Chapter 11, Section 11.4.2, Illustration 5;
5. sale of stolen data/stolen property.

1.5.18 Computer Network Intrusions

Computer Networks pose a problem by way of security threat because people can get into them from anywhere. The popular movie “War Games” illustrated an extreme but useful example of this. “Crackers” who are often misnamed “Hackers”^[11] can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords. Network intrusions are illegal, but detection and enforcement are difficult. Current laws are limited and many intrusions go undetected.

The cracker can bypass existing password protection by creating a program to capture logon IDs and passwords. The practice of “strong password” is therefore important (password strength is explained in Chapter 4). Importance of passwords and password rules is explained in Chapter 11 (Network Security in Perspective) in Ref. #3, Books, Further Reading. In Ref. #3, Books, Chapter 35 (Auditing for Security) explains about password cracking tools in the context of vulnerability scanning and penetration testing. Refer to Ref. #3, Books, Chapter 17 (Security of Wireless Networks and Box 17.3 in particular) for crackers and hackers and Chapter 14 (Intrusion Detection for Securing Networks) for Trojans.

1.5.19 Password Sniffing

Password Sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site. Whoever installs the Sniffer can then impersonate an authorized user

and login to access restricted documents. Laws are not yet set up to adequately prosecute a person for impersonating another person online. Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs. “Password cracking” and “password sniffing” are explained in Chapter 4.

1.5.20 Credit Card Frauds

Information security requirements for anyone handling credit cards have been increased dramatically recently. Millions of dollars may be lost annually by consumers who have credit card and calling card numbers stolen from online databases. Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information. Bulletin boards and other online services are frequent targets for hackers who want to access large databases of credit card information. Such attacks usually result in the implementation of stronger security systems. For more on credit card frauds see Chapter 3, Section 3.4 (Credit Card Frauds in Mobile and Wireless Computing Era) in Ref. #1, Books, Further Reading. Security of cardholder data has become one of the biggest issues facing the payment card industry. Payment Card Industry Data Security Standard (PCI-DSS) is a set of regulations developed jointly by the leading card schemes to prevent cardholder data theft and to help combat credit card fraud. We urge readers to visit the PCI-DSS-related URLs.^[16] Refer to Chapter 11, Section 11.4.2.

1.5.21 Identity Theft

Identity theft is a fraud involving another person’s identity for an illicit purpose. This occurs when a criminal uses someone else’s identity for his/her own illegal purposes. Phishing and identity theft are related offenses (the topic is addressed in Chapter 5). Examples include fraudulently obtaining credit, stealing money from the victim’s bank accounts, using the victim’s credit card number (recall the discussion in the previous section

Box 1.5 \ Spam in Cyberworld

Basically, “Spam” is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. Although the most widely recognized form of Spam is E-Mail Spam, this term is applied to similar abuses in other media: instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions and file sharing network Spam. Spam is caused by flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Often, this may result in the notorious DoS attack. Commercial advertising often happens to be the cause of Spam. Such advertisements are often for products of dubious reputation and fraud schemes meant to make people believe they can get rich overnight! Some Spam may also get generated through quasi-legal services. Spam hardly costs much to the sender; most of the costs are paid for by the recipient or the carriers rather than by the sender.

People who engage in the activity of electronic Spam are called spammers. Two main types of Spam are worth mentioning: “cancelable Usenet Spam” in which a single message is sent to several Usenet newsgroups and “E-Mail Spam” which targets individual users with direct mail messages. Often, spammers create E-Mail Spam lists by scanning Usenet postings, by stealing Internet mailing lists or searching the Web for addresses. Typically, it costs money to users if they receive E-Mail Spam. Any person with measured phone service can read or receive their mail. Spam does not cost much to people. Spam does, however, cost money to ISPs and to online service providers to transmit Spam. Unfortunately, subscribers end up paying these costs because the costs are transmitted directly to subscribers.

For further details, refer to Ref. #3 (Chapter 11, Denial-of-Service attacks, p. 177), Books, Further Reading.

about credit card frauds), establishing accounts with utility companies, renting an apartment or even filing bankruptcy using the victim's name. The cyberimpersonator can steal unlimited funds in the victim's name without the victim even knowing about it for months, sometimes even for years!

Thus far, we have provided an overview of various types of well-known cybercrimes. In most cybercrime forms, computers and/or other digital devices end up getting used as one or a combination of the following:

1. As the tool for committing cybercrime;
2. crime involving attack against the computer;
3. use for storing information related to cybercrime/information useful for committing cybercrime.

1.6 Cybercrime: The Legal Perspectives

Greater details on this are discussed in Chapter 6 and only a brief discussion is done in this section. Cybercrime poses a mammoth challenge. In the first comprehensive presentation of computer crime, *Computer Crime: Criminal Justice Resource Manual* (1979) (see Ref. #2, Additional Useful Web References, Further Reading), computer-related crime was defined in the broader meaning as: *any illegal act for which knowledge of computer technology is essential for a successful prosecution*. International legal aspects of computer crimes were studied in 1983. In that study, computer crime was consequently defined as: *encompasses any illegal act for which knowledge of computer technology is essential for its perpetration*.

Cybercrime, in a way, is the outcome of "globalization." However, globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of trans-national offenses. The network context of cybercrime makes it one of the most globalized offenses of the present and the most modernized threats of the future. This problem can be resolved in two ways. One is to divide information systems into segments bordered by state boundaries (cross-border flow of information). The other is to incorporate the legal system into an integrated entity obliterating these state boundaries. Apparently, the first way is unrealistic. Although all ancient empires including Rome, Greece and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems cannot be an imagined practice. In a globally connected world, information systems become the unique empire without tangible territory.

1.7 Cybercrimes: An Indian Perspective

India has the fourth highest number of Internet users in the world. According to the statistics posted on the site (<http://www.iamai.in/>), there are 45 million Internet users in India, 37% of all Internet accesses happen from cybercafes and 57% of Indian Internet users are between 18 and 35 years. The population of educated youth is high in India. It is reported that compared to the year 2006, cybercrime under the Information Technology (IT) Act recorded a whopping 50% increase in the year 2007.^[17] A point to note is that the majority of offenders were under 30 years. The maximum cybercrime cases, about 46%, were related to incidents of cyberpornography, followed by hacking. In over 60% of these cases, offenders were between 18 and 30 years, according to the "Crime in 2007" report of the National Crime Record Bureau (NCRB). Box 1.6 shows the Indian Statistics on cybercrimes. Also revisit Tables 1.1–1.4.

The Indian Government is doing its best to control cybercrimes. For example, Delhi Police have now trained 100 of its officers in handling cybercrime and placed them in its Economic Offences Wing. As at the time of writing this, the officers were trained for 6 weeks in computer hardware and software, computer networks comprising data communication networks, network protocols, wireless networks and network security.

Box 1.6 Cybercrimes: Indian Statistics

(A) Cybercrimes: Cases of Various Categories under ITA 2000

217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year (2006), thereby reporting an increase of 52.8% in 2007 over 2006. 22.3% cases (49 out of 217 cases) were reported from Maharashtra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each).

45.6% (99 cases) of the total 217 cases registered under ITA 2000 were related to obscene publication/transmission in electronic form, known as cyberpornography. 86 persons were arrested for committing such offenses during 2007. There were 76 cases of hacking with computer system during the year wherein 48 persons were arrested. Out of the total (76) hacking cases, the cases relating to loss/damage of computer resource/utility under Section 66(1) of the IT Act were 39.5% (30 cases) whereas the cases related to hacking under Section 66(2) of IT Act were 60.5% (46 cases).

Maharashtra (19) and Kerala (4) registered maximum cases under Section 66(1) of the IT Act out of total 30 such cases at the National level. Out of the total 46 cases relating to hacking under Section 66(2), most of the cases (31) were reported from Karnataka followed by Kerala (7) and Andhra Pradesh (3). 29.9% of the 154 persons arrested in cases relating to ITA 2000 were from Maharashtra (46) followed by Karnataka and Madhya Pradesh (16 each). The age-wise profile of persons arrested in cybercrime cases under ITA 2000 showed that 63.0% of the offenders were in the age group 18–30 years (97 out of 154) and 29.9% of the offenders were in the age group 30–45 years (46 out of 154). Tamil Nadu reported two offenders whose ages were below 18 years.

India is said to be the "youth country" given the population age distribution. From the potential resources perspective, this is supposed to be a great advantage; assuming that these youths will get appropriate training to develop the required professional skills in them. However, from cyber-crime perspective, this youth aspect does not seem good as revealed by cybercrime statistics in India. Crime head-wise and age-group-wise profile of the offenders arrested under ITA 2000 revealed that 55.8% (86 out of 154) of the offenders were arrested under "Obscene publication/transmission in electronic form" of which 70.9% (61 out of 86) were in the age group 18–30 years. 50% (24 out of 48) of the total persons arrested for "Hacking with Computer Systems" were in the age group of 18–30 years.

(B) Cybercrimes: Cases of Various Categories under IPC Section

A total of 339 cases were registered under IPC Sections during the year 2007 as compared to 311 such cases during 2006, thereby reporting an increase of 9.0%. Madhya Pradesh reported maximum number of such cases, nearly 46.6% of total cases (158 out of 339) followed by Andhra Pradesh 15.6% (53 cases) and Chhattisgarh 15.3% (52 cases). Majority of the crimes out of total 339 cases registered under IPC fall under two categories, viz., Forgery (217) and Criminal Breach of Trust or Fraud (73). Although such offenses fall under the traditional IPC crimes, these cases had the cyberovertones wherein computer, Internet or its enabled services were present in the crime and hence they were categorized as Cybercrimes under IPC. The cyberforgery (217 cases) accounted for 0.33% out of the 65,326 cases reported under cheating. The cyberfrauds (73) accounted for 0.47% of the total Criminal Breach of Trust cases (15,531).

The cyberforgery cases were the highest in Madhya Pradesh (133) followed by Chhattisgarh (26) and Andhra Pradesh (22). The cases of cyberfraud were highest in Madhya Pradesh (20) followed by Punjab (17) and Andhra Pradesh (15). A total of 429 persons were arrested in the country for Cybercrimes under IPC during 2007. 61.5% offenders (264) of these were taken into custody for offenses under "Cyberforgery," 19.8% (85) for "Criminal Breach of Trust/Fraud" and 11.4% (49) for "Counterfeiting Currency/Stamps."

States such as Madhya Pradesh (166), Andhra Pradesh (83), Chhattisgarh (82) and Punjab (69) have reported higher arrests for cybercrimes registered under IPC. The age-group-wise profile of the arrested persons showed that 55.2% (237 of 429) were in the age group of 30–45 years and 29.4% (126 of 429) of the offenders were in the age group of 18–30 years. Only four offenders from Chhattisgarh were below 18 years of age. Crime head-wise and age-wise profile of the offenders arrested under Cybercrimes (IPC) offenders involved in forgery cases were more in the age group of 30–45 (54.9%, 145

Box 1.6 Cybercrimes: . . . (Continued)

of 264). 57.6% of the persons arrested under Criminal Breach of Trust/Cyberfraud offenses were in the age group 30–45 years (49 out of 85).

(C) Incidence of Cybercrimes in Cities

17 out of 35 mega cities did not report any case of cybercrime (neither under the IT Act nor under IPC Sections) during the year 2007. A total of 17 mega cities have reported 118 cases under IT Act and 7 mega cities reported 180 cases under various sections of IPC. There was an increase of 32.6% (from 89 cases in 2006 to 118 cases in 2007) in cases under IT Act as compared to previous year (2006), and an increase of 26.8% (from 142 cases in 2006 to 180 cases in 2007) of cases registered under various sections of IPC. Bengaluru (40), Pune (14) and Delhi (10) have reported high incidence of cases (64 out of 118 cases) registered under IT Act, accounting for more than half of the cases (54.2%) reported under the Act. Bhopal has reported the highest incidence (158 out of 180 cases) of cases reported under IPC sections accounting for 87.8%.

1.8 Cybercrime and the Indian ITA 2000

In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in January 30, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step toward the Law relating to E-Commerce at international level to regulate an alternative form of commerce and to give legal status in the area of E-Commerce. It was enacted taking into consideration UNICITRAL model of Law on Electronic Commerce (1996).^[18]

1.8.1 Hacking and the Indian Law(s)

Cybercrimes are punishable under two categories: the ITA 2000 and the IPC (see Tables 1.1 and 1.2). A total of 207 cases of cybercrime were registered under the IT Act in 2007 compared to 142 cases registered in 2006. Under the IPC too, 339 cases were recorded in 2007 compared to 311 cases in 2006. There are some noteworthy provisions under the ITA 2000, which is said to be undergoing key changes very soon (as at the time of writing this, Table 1.7).

Table 1.7 | The key provisions under the Indian ITA 2000 (before the amendment)

<i>Section Ref. and Title</i>	<i>Chapter of the Act and Title</i>	<i>Crime</i>	<i>Punishment</i>
Sec. 43 (Penalty for damage to computer, computer system, etc.)	CHAPTER IX Penalties and Adjudication	Damage to computer system, etc.	Compensation for ₹ 1 crore (₹ 10,000,000).
Sec. 66 (Hacking with computer system)	CHAPTER XI Offences	Hacking (with intent or knowledge).	Fine of ₹ 2 lakhs (₹ 200,000) and imprisonment for 3 years.
Sec. 67 (Publishing of information which is obscene in electronic form)	CHAPTER XI Offences	Publication of obscene material in electronic form.	Fine of ₹ 1 lakh (₹ 100,000), imprisonment of 5 years and double conviction on second offence.

(Continued)

Table 1.7 | (Continued)

<i>Section Ref. and Title</i>	<i>Chapter of the Act and Title</i>	<i>Crime</i>	<i>Punishment</i>
Sec. 68 (Power of controller to give directions)	CHAPTER XI Offences	Not complying with directions of controller.	Fine up to ₹ 2 lakhs (₹ 200,000) and imprisonment of 3 years.
Sec. 70 (Protected system)	CHAPTER XI Offences	Attempting or securing access to computer of another person without his/her knowledge.	Imprisonment up to 10 years.
Sec. 72 (Penalty for breach of confidentiality and privacy)	CHAPTER XI Offences	Attempting or securing access to computer for breaking confidentiality of the information of computer.	Fine up to ₹ 1 lakh (₹ 100,000) and imprisonment up to 2 years.
Sec. 73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	CHAPTER XI Offences	Publishing false digital signatures, false in certain particulars.	Fine of ₹ 1 lakh (₹ 100,000) or imprisonment of 2 years or both.
Sec. 74 (Publication for fraudulent purpose)	CHAPTER XI Offences	Publication of Digital Signatures for fraudulent purpose.	Imprisonment for the term of 2 years and fine of ₹ 1 lakh (₹ 100,000).

Source: Information Technology Act 2000, Act no. 21, accessible at the URL: http://www.commonlii.org/in/legis/num_act/ita2000258/ (22 February 2000).

Box 1.7 Hacking and the ITA 2008

The number of Offenses to be monitored has increased. According to cyberlaw experts, "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime." Cases of Spam, hacking, cyberstalking and E-Mail fraud are rampant and, although cybercrimes cells have been set up in major cities, the problem is that most cases remain unreported due to a lack of awareness. In a milieu like this, there are a number of pertinent questions in the minds of a commoner: When can consumers approach a cybercrime cell? What should the victims do? How does one maintain security online?

Any and every incident of cybercrime involving a computer or electronic network can be reported to a police station, irrespective of whether it maintains a separate cell or not. CHAPTER XI of the original ITA 2000 lists a number of activities that may be taken to constitute cybercrimes. This includes tampering with computer source code, hacking, publishing or transmitting any information in electronic form that is lascivious, securing access to a protected system, and breach of confidentiality and privacy. In the original ITA 2000, the following is stated under CHAPTER XI (Offences):

1. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
2. Whoever commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to ₹ 2 lakhs (₹ 200,000), or with both.

Box 1.7 Hacking . . . (Continued)

In the amendment to the IT Act 2000, now known as the ITA 2008, several offenses have been added to the Act. The amendments have now revealed a whole bundle of surprises which will make the cybercrime police jump. Existing Sections 66 and 67 (in the original ITA 2000) on hacking and obscene material have been updated by dividing them into more crime-specific subsections, thereby making cybercrimes punishable.

In Section 66, hacking as a term has been removed. This section has now been expanded to include Sections 66A (offensive messages), 66B (receiving stolen computer), 66C (identity theft), 66D (impersonation), 66E (voyeurism) and 66F (cyberterrorism). Section 66F is a new section of the ITA 2008 (recent amendments to the Indian ITA 2000). It covers "Cyberterrorism" and makes it punishable with imprisonment up to life term. This may cover hacking, DoS attacks, Port Scanning, spreading viruses, etc., if it can be linked to the object of terrorizing people. Conspiracy is also covered under the section. The offense is not bailable or compoundable. Refer to Chapter 4 to know more on computer viruses.

1.9 A Global Perspective on Cybercrimes

Cybercrime definitions were provided in Section 1.2. As mentioned there, statute and treaty law both refer to cybercrime. In Australia, cybercrime has a narrow statutory meaning as used in the *Cyber Crime Act 2001*, which details offenses against computer data and systems. However, a broad meaning is given to cybercrime at an international level. In the Council of Europe's (CoE's) *Cyber Crime Treaty*, cybercrime is used as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copyright offenses. This wide definition of cybercrime overlaps in part with general offense categories that need not be Information & Communication Technology (ICT)-dependent, such as white-collar crime and economic crime. Figure 1.13 shows countries taking actions against Spam. Although this status is from the International Telecommunication Union (ITU) survey conducted in 2005, we get an idea about the global perspective. The status on E-Mail Spam legislation by country is available at the site http://en.wikipedia.org/wiki/E-mail_spam_legislation_by_country (29 January 2010). ITU activities on countering Spam can be read by visiting the link www.itu.int/spam (8 May 2010).

The Spam legislation scenario mentions "none" about India as far as E-Mail legislation in India is concerned. The legislation refers to India as a "loose" legislation, although there is a mention in Section 67 of Indian ITA 2000. See Table 1.7.

About 30 countries have enacted some form of anti-Spam legislation (see Fig. 1.13). There are also technical solutions by ISPs and end-users. However, in spite of this, so far there has been no significant impact on the volume of Spam with spammers sending hundreds of millions of messages per day. The growing phenomenon is the use of Spam to support fraudulent and criminal activities – including attempts to capture financial information (e.g., account numbers and passwords) by masquerading messages as originating from trusted companies ("brand-spoofing" or "Phishing") – and as a vehicle to spread viruses and worms. On mobile networks, a peculiar problem is that of sending of bulk unsolicited text messages aimed at generating traffic to premium-rate numbers. As there are no national "boundaries" to such crimes under cybercrime realm, it requires international cooperation between those who seek to enforce anti-Spam laws.

Thus, one can see that there is a lot to do toward building confidence and security in the use of ICTs and moving toward international cooperation agenda. This is because in the 21st century, there is a growing dependency on ICTs that span the globe. There was a rapid growth in ICTs and dependencies that led to shift in perception of cybersecurity threats in mid-1990s. The linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have began assessment of threats,

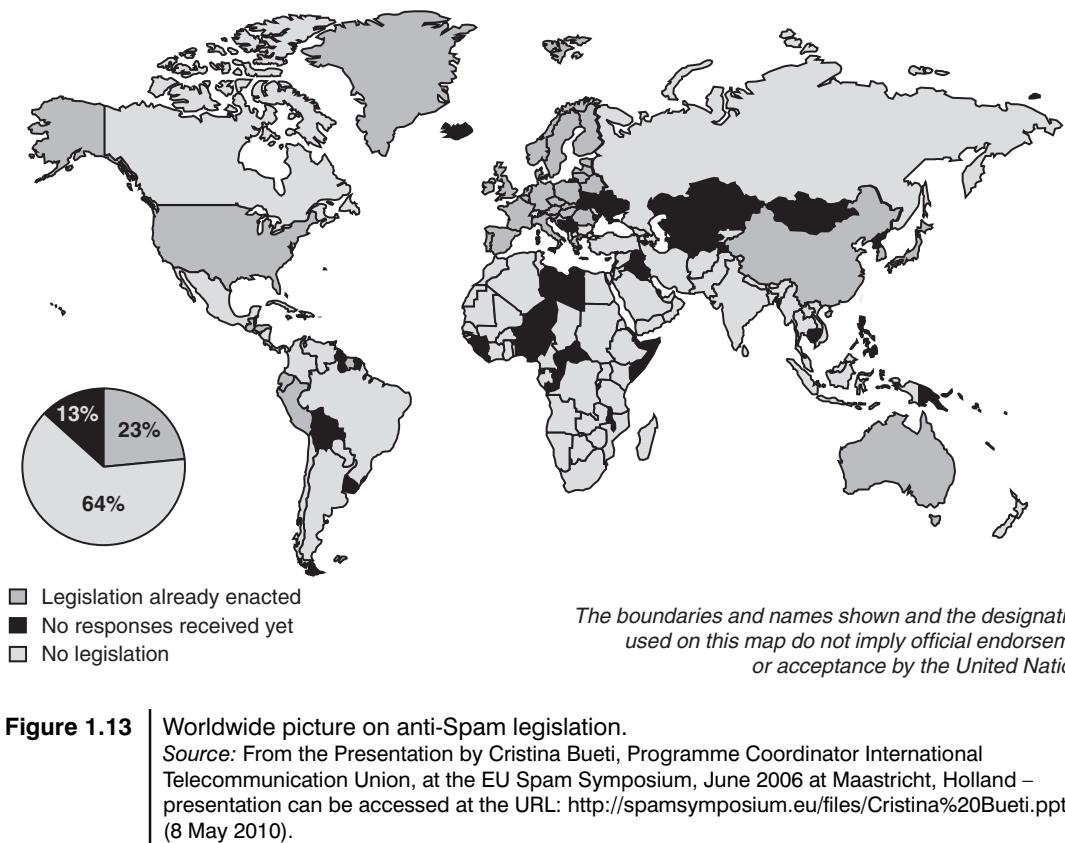


Figure 1.13 Worldwide picture on anti-Spam legislation.

Source: From the Presentation by Cristina Bueti, Programme Coordinator International Telecommunication Union, at the EU Spam Symposium, June 2006 at Maastricht, Holland – presentation can be accessed at the URL: <http://spamsymposium.eu/files/Cristina%20Bueti.ppt#1> (8 May 2010).

vulnerabilities and started exploring mechanisms to redress them. Recently, there have been a number of significant developments such as

1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime. The convention targets hackers, those spreading destructive computer viruses (refer to Chapter 4), those using the Internet for the sexual exploitation of children or the distribution of racist material, and terrorists attempting to attack infrastructure facilities or financial institutions. The Convention is in full accord with all the US constitutional protections, such as free speech and other civil liberties, and will require no change to the US laws.
2. In August 18, 2006, there was a news article published “ISPs Wary About ‘Drastic Obligations’ on Web Site Blocking.” European Union (EU) officials want to debar suspicious websites as part of a 6-point plan to boost joint antiterrorism activities. They want to block websites that incite terrorist action. Once again it is underlined that monitoring calls, Internet and E-Mail traffic for law enforcement purposes is a task vested in the government, which must reimburse carriers and providers for retaining the data.
3. CoE Cyber Crime Convention (1997–2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.^[19] More than 40 countries have ratified the Convention to date.

One wonders as to what is the role of business/private sector in taking up measures to prevent cybercrime and toward responsibilities and role related to the ownership of information and communication infrastructures. Effective security requires an in-depth understanding of the various aspects of information and communication networks. Therefore, private sector's expertise should be increasingly involved in the development and implementation of a country's cybersecurity strategy.

1.9.1 Cybercrime and the Extended Enterprise

It is a continuing problem that the average user is not adequately educated to understand the threats and how to protect oneself. Actually, it is the responsibility of each user to become aware of the threats as well as the opportunities that "connectivity" and "mobility" presents them with. This aspect is emphasized in Chapter 3. In this context, it is important to understand the concept of "extended enterprise." This term (Fig. 1.14) represents the concept that a company is made up not just of its employees, its board members and executives, but also its business partners, its suppliers and even its customers. The extended enterprise can only be successful if all of the component groups and individuals have the information they need in order to do business effectively. An extended enterprise is a "loosely coupled, self-organizing network" of firms that combine their economic output to provide "products and services" offerings to the market. Firms in the extended enterprise may operate independently, for example, through market mechanisms or cooperatively through agreements and contracts. To understand information security in the extended enterprise paradigm, refer to Chapter 1, Ref. #3, Books, Further Reading.

Seamless flow of "information" to support instantaneous "decision-making ability" (as envisaged in Bill Gates' *Business@the Speed of Thought*) is crucial for the "external enterprise." This becomes possible through the "interconnectedness." Due to the interconnected features of information and communication technologies, security overall can only be fully promoted when the users have full awareness of the existing threats and dangers. Governments, businesses and the international community must, therefore, proactively help users' access information on how to protect themselves.

Given the promises and challenges in the extended enterprise scenario, organizations in the international community have a special role in sharing information on good practices, and creating open and accessible enterprise information flow channels for exchanging of ideas in a collaborative manner. International cooperation at the levels of government, industry, consumer, business and technical groups to allow a global and coordinated approach to achieving global cybersecurity is the key.

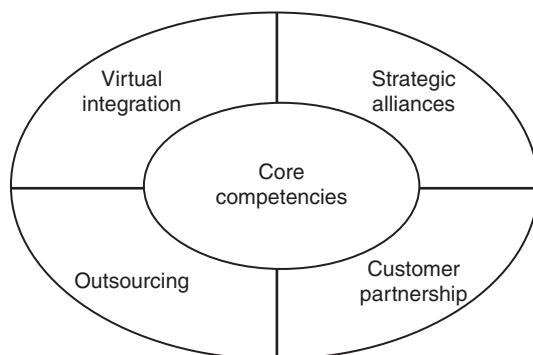


Figure 1.14 | Extended enterprise.

1.10 Cybercrime Era: Survival Mantra for the Netizens

The term “Netizen” was coined by Michael Hauben. Quite simply, “Netizens” are the Internet users. Therefore, by corollary, “Netizen” is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms). The 5P Netizen mantra for online security is: (a) Precaution, (b) prevention, (c) Protection, (d) Preservation and (e) Perseverance. For ensuring cybersafety, the motto for the “Netizen” should be “Stranger is Danger!” If you protect your customer’s data, your employee’s privacy and your own company, then you are doing your job in the grander scheme of things to regulate and enforce rules on the Net through our community. [Refer to Chapters 29–31, Ref. #3, Books, Further Reading for a detailed discussion on the topic of “privacy” and its impact on business as well as technological impact on privacy (RFID, Software Agents, Smart Cards, etc.).] Refer to Part I of Appendix D (in CD).

NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once. This is the reason they have established cyberlabs across major cities in India (Ref. #6, Additional Useful Web References, Further Reading). More importantly, users must try and save any electronic information trail on their computers. That is all one can do until laws become more stringent or technology more advanced. Refer to Appendices U and V (in CD).

Some agencies have been advocating for the need to address protection of the Rights of Netizens. There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO-like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police. There are also a few incidents where Police have pursued false cases on innocent IT professionals. The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time. Chapter 6 addresses further details on the Indian ITA 2000 and its subsequent amendments in the year 2008.

1.11 Concluding Remarks and Way Forward to Further Chapters

This chapter sets the context for the rest of the book; in that sense, this is a “curtain raiser” chapter. Having provided a broad overview about cybercrime, in the subsequent chapters reader will be taken through other key aspects of cybercrime: how the crimes are planned, the tools and methods used for launching the attacks, light on legal aspects of cybercrime, cyberforensics, social as well as psychological and ethical dimensions of cybercrime, organizational implications, career implications, etc. Chapter 11 has extensive illustrations on cybercrime. For the reasons of confidentiality and protection of individual privacy, the names and other details are masked; however the scenarios are real. If there happens to exist any individual by the name mentioned, living or deceased, then it would be a pure coincidence. A key message, as we end this chapter, is for the ethical hacking community; while some people argue that there should be no such term as “ethical hacking” because there cannot be anything ethical about hacking, the need for and availability of professional certifications such as “Certified Ethical Hacking” is purely for investigative nature. Even such individuals who work on commercial terms when invited to hack systems for vulnerability assessment, should remember that their job is highly onerous and that they should bear in mind their ethical responsibility all the time. These aspects are explained in Chapter 35, Ref. #3, Books, Further Reading.

SUMMARY

Cyberspace is one of the great legal frontiers of our time. Cybercrime is a term which is used to describe the act in which computers and networks are targeted for criminal activity. Such crimes have emerged as a new class of crimes, rapidly increasing due to extensive use of the Internet and IT-enabled services. We learnt in this chapter that there are many types of computer-related crimes. Cybercrimes range from tampering with computer documents, hacking and

cyberpornography to false electronic evidence, unauthorized access to protected computer documents and breach of confidentiality. Within India and worldwide, there has been a phenomenal rise in the incidents of cybercrime. The issue of cybercrime continues to grow as a controversy for several reasons. We need laws that protect us from computer crimes, but we also need laws that are not so controlling that they compromise our civil liberties and constitutional rights.

REVIEW QUESTIONS

1. What is cybercrime? How do you define it?
2. How do we classify cybercrimes? Explain each one briefly.
3. What are the different types of cybercriminals?
4. Is there a difference between “cybercrime” and “cyberfraud”? Explain.
5. How do viruses get disseminated? Explain with diagrams.
6. Write a short note on “Indian Legal Perspective on Cybercrime.” You may like to augment your note using your own research, in addition to the material presented in this chapter.
7. How do you think cybercrime has relevance in the extended enterprise context? Explain.
8. Explain in your own words what you understand about the global cooperation required in fighting against cybercrime.

REFERENCES

- [1] *Information Security Glossary* can be visited at: http://www.yourwindow.to/information-security/gl_cybercrime.htm (14 March 2009).
- [2] <http://qanda.encyclopedia.com/question/cybernetics-related-84610.html> (2 February 2009).
- [3] <http://www.pangaro.com/published/cyber-macmillan.html> (26 February 2009).
- [4] <http://www.catunesco.upc.es/ads/beer.pdf> (26 February 2009).
- [5] http://www.gwu.edu/~asc/cyber_definition.html (26 February 2009).
- [6] <http://en.wikipedia.org/wiki/Cybernetics> (20 February 2009).
- [7] Site for *Information Technology Act 2000 Amendment* can be visited at: <http://cybercrime.planetindia.net/new-cyber-security-infrastructure.htm> (14 March 2009).
- [8] 2008 CSI Computer Crime and Security Survey can be assessed at: <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf> (15 March 2009).
- [9] Israeli Trojan Horse scandal can be visited at: <http://www.msnbc.msn.com/id/8064757/> (18 March 2009).
- [10] To understand the technical details involved in W32.Myfp.A, visit the technical document available at: <http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf> (12 February 2009).
- [11] Loza, B. <http://www.safepatrolsolutions.com/papers/Crackers.pdf> (1 February 2010).

- [12] Find out more on Children's Online Privacy Protection Act (COPPA) in the following links:
 COPPA FAQS – <http://www.ftc.gov/privacy/coppafaqs.shtm> (13 March 2009).
 COPPA Compliance – <http://www.coppa.org/comply.htm> (13 March 2009).
 The official COPPA website coming up soon, visit the site at: <http://www.mccoppa.co.uk/home1/index.html> (13 March 2009).
 Another good site on COPPA – <http://epic.org/privacy/kids/> (13 March 2009).
- [13] To know about *Net-Nanny* and *Cybersitter*, visit the following links:
Net-Nanny
<http://www.netnanny.com/competition> (2 February 2010).
<http://www.netnanny.com/> (2 February 2010).
<http://internet-filter-review.toptenreviews.com/netnanny-review.html> (2 February 2010).
<http://personalweb.about.com/cs/viewingsites/a/403siteblocking.htm> (2 February 2010).
Cybersitter
<http://cexx.org/censware.htm> (How to Disable Internet Filtering Programs) (5 February 2010).
http://www.yourwindow.to/information-security/gl_cybersitter.htm (5 February 2010).
- [14] For *global software piracy scenario*, readers can refer the reports in the following links:
Fourth Annual BSA and IDC Global Software Piracy Study. <http://www.ifap.ru/library/book184.pdf> (2 March 2009).
 (Software) piracy. <http://w3.bsa.org/global-study/> (10 February 2010).
 2006 IDC Report on Software Piracy. http://www.adobe.com/de/aboutadobe/antipiracy/pdfs/IDC_Piracy_Study_REPORT.pdf (12 February 2009).
- [15] To know more about Y2K viruses, visit: <http://www.kumite.com/myths/opinion/thoughts/1999/y2kvirus.htm> (2 February 2010).
- [16] To know about *PCI DSS (Payment Card Industry Data Security Standard)*, visit the following links:
PCI DSS FQAs (frequently asked questions and myths). <http://www.pcicomplianceguide.org/pcifaqs.php> (12 April 2009).
- Visit this page for the standard. <http://www.scribd.com/doc/6486863/PCI-DSS-v-12> (11 April 2009).
 To understand the difference between the latest version of PCI-DSS and the older version, visit:
 PCI DSS version 1.1 and 1.2 differences and updates. http://www.pacifica.ru/download/pci_dss/pci_dss_summary_of_changes_v1-2.pdf (12 April 2009).
http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1326025,00.html (10 April 2009).
- [17] http://economictimes.indiatimes.com/Internet/_Cyber_crimes_record_50_per_cent_jump_in_India/articleshow/3855662.cms (3 March 2009).
- [18] Following links can be referred for the *UNCITRAL Model Law on Electronic Commerce*
[http://www.genghinieassociati.it/acrobat/it%20security/Leggi/UNCITRAL%20Model%20Law%20on%20Electronic%20Commerce%20\(English\).PDF](http://www.genghinieassociati.it/acrobat/it%20security/Leggi/UNCITRAL%20Model%20Law%20on%20Electronic%20Commerce%20(English).PDF) (16 August 2009).
http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf (16 August 2009).
<http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> (16 August 2009).
UNCITRAL-Model-Law-on-Electronic_Signatures-with-GuideToEnactment_2001 (16 August 2009).
<http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/> (16 August 2009).
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (16 August 2009).
- [19] Schjølberg, S. and Hubbard, A.M. (2005) *Harmonizing National Legal Approaches on Cybercrime*, International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, 28 June–1 July 2005, Geneva, Document: CYB/04 Dated 10 June 2005.
http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (3 March 2009).

FURTHER READING

Additional Useful Web References

1. NASSCOM, Types of Cybercrimes, visit: <http://www.indiacyberlab.in/cybercrimes/types.htm> (22 February 2009).
2. SRI International for the US Department of Justice (1979) *The Criminal Justice Resource Manual on Computer Crime*, Menlo Park, CA, USA.
3. Ibid, p. 3.
4. Schjolberg, S. (1983) *Computers and Penal Legislation – A Study of the Legal Politics of a new Technology*, CompLex 3/86, Universitetsforlaget, Norway.
5. The Indian ITA 2000, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN010239.pdf> (22 February 2009).
6. NASSCOM, www.INDIACYBERLAB.in — <http://www.indiacyberlab.in/news/190706.htm>
7. India occupies the 3rd position in the world in terms of mobile phone usage, visit: <http://www.expressindia.com/news/fullstory.php?newsid=61762> (28 January 2010).
8. For detailed statistics on growth of cybercrimes in India, visit: http://cybercrime.planetindia.net/bytoby_byte.htm (1 March 2009).
9. To understand the Indian Position on Cyber Defamation, visit: <http://jurisonline.in/2009/11/cyber-defamation-%E2%80%93-position-in-india/> (29 January 2010).
10. Visit Law website at: <http://www.findlaw.com/scripts/search.pl?CiRestriction=cyberterrorism>
11. The Terrorism research center, <http://www.terrorism.com/>

As quoted at: http://terrorism.about.com/od/whatisterrorism/ss/DefineTerrorism_6.htm (25 March 2010), FBI definition “*Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.*” Department of State definition: “*The term ‘terrorism’ means premeditated, politically motivated violence*

perpetrated against noncombatant targets by sub national groups or clandestine agents.”
12. Martinez, S.M. FBI Report on *Trends and Developments in Cyber Crime in the Information Age*, <http://www.adbi.org/files/2005.09.07.cpp.trends.cybercrime.presentation.pdf> (27 March 2009).
13. Denning, D.E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* can be accessed at: <http://www.nautilus.org/info-policy/workshop/papers/denning.html>
14. Borland, J. *Analyzing the Threat Of Cyberterrorism*, TechWeb News, <http://www.techweb.com/wire/story/TWB19980923S0016>
15. Verton, D. *Are cyberterrorists for real?* Federal Computer Week, <http://www.fcw.com/fcw/articles/2000/0626/pol-terror-06-26-00.asp>
16. Hacked Sites Archive can be visited at: http://www.2600.com/hacked_pages/ (6 March 2009).
17. The following link shows how certain sites were hacked for a website hacked by a Turkish Hacker. http://www.youtube.com/watch?v=_2dNz2TUhpk
http://search.yahoo.com/search?p=examples+of+websites+hacked+by+hackers&ei=UTF-8&fr=msgr-buddy&xargs=0&pstart=1&b=11&xa=XOcfu0P0c_8YS_U8TQak_g--,1236412181
18. To know what *hacking software* is, visit: <http://www.hackingalert.com/hacking-articles/free-hacking-program.php> (6 March 2009).

The entire *hacking panorama* is explained here – topics such as: *Computer Hacking, Basics of Hacking, Hacking Tutorial, History of Hacking, Hackers and Crackers, Catching a Hacker, Hacking Culture, Employee Internet Policy*
19. The Ponemon Institute (2009) Survey done on the *Business Risk of a Lost Laptop* (A Study of US IT Practitioners), visit: <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/The%20Business%20Risk%20of%20a%20Lost%20Laptop%20Final%201.pdf> (1 February 2010).

20. To know about *Online Gambling* in India, visit the following links:

<http://answers.google.com/answers/threadview?id=294632> (1 February 2010).

<http://www.onlinecasinoreports.in/facts.php> (1 February 2010).

<http://www.onlinecasinoreports.in/articles/2009/12/24/india-online-gambling-review-2009.php> (1 February 2010).

21. For Tips on how to protect your child on the Internet, visit: <http://www.indiacyberlab.in/cyberkids/index.html> (13 March 2009).

22. The SC Magazine has published the story about NASA site attack by hackers through the use of SQL injection. To know more on this, visit: <http://www.scmagazineus.com/nasa-sites-hacked-via-sql-injection/article/159181/> (1 February 2010).

23. To understand about *Cybercafes under ITA 2008* (ITA 2008 is the Indian IT Act 2000 amended), visit: http://www.naavi.org/cl_editorial_09/edit_jan07_itaa_analysis_7_cyber_cafe.htm (14 March 2009).

24. To understand views on whether the Amended ITA 2000 (ITA 2008) is stringent enough for cybercriminals, visit: <http://cybercrime.planet-india.net/ita-08-more-stringent-00.htm> (19 March 2009).

25. Information on *Cyber Crime Police Stations in Different States of India* (telephone numbers and E-Mail addresses of contact personnel) can be found in: <http://infosecawareness.in/cyber-crime-cells-in-india/> (17 March 2009).

26. For Indian numbers on Internet connections, mobile phone usage, etc., visit:
<http://www.medianama.com/2008/10/223-quarterly-india-internet-mobile-numbers-and-a-wireless-internet/> (17 March 2009).

<http://www.watblog.com/statistics-internet-and-mobile/> (17 March 2009).

<http://interneththought.blogspot.com/2008/03/mobile-growth-in-india-is-something.html> (17 March 2009).

According to the article at the links just mentioned above, there is something different about the growth of mobile computing in India. Statistics on Indian Mobile Users' Internet Usage can be visited at the following link: <http://trak.in/tags/business/2008/05/20/indian-top-10-mobile-sites/> (15 March 2009).

To know more about India's Internet Market Statistics (2001–2010), visit: http://www.reportbuyer.com/telecoms/broadband/india_internet_market_statistics_2001_2010.html (2 March 2009).

27. To find out another way of cybercrime classification, visit: <http://www.b4usurf.org/index.php?page=types-of-cybercrime> (21 March 2009).
28. For the full Defense *Paper on Information Warfare*, visit: <http://cryptome.org/iwdmain.htm> (12 April 2009).
29. Read article *Namesake Cybersquatting, An IPR Evil* at: <http://www.legalserviceindia.com/articles/namesake.htm>

Books

- Godbole, N. (2009) Chapter 3 (Section 3.11), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
- ibid, Appendix AI – Cybercrime and Information Security.
- ibid, Chapters 1, 11, 14, 17, 29–31, 32, 35 and 38.
- ibid, pp 64, 167, 260 (viruses and worms).
- ibid Chapter 1 (Information Systems in Global Context) and Chapter 18 (Business Applications Security: An EAI Perspective) – for understanding the extended enterprise context for cyber crime and security.
- Jain, N.C. (2008) *Cyber Crime*, 1st edn, Allahabad Law Agency, Faridabad.
- Gregory, K. (2007) *Wireless Crime and Forensic Investigation*, Auerbach Publication, New York.
- Bryant, R.P. (2008), *Investigating Digital Crime*, Wiley.

9. Denning, D.E. (1999) *Information Warfare and Security*, Addison-Wesley.
10. Bologna, G.J. and Shaw, P. (2000) *Avoiding Cyber Fraud in Small Businesses: What Auditors and Owners Need to Know*, Wiley.
11. Mehta, R. and Mehta R. *Credit Cards: A Legal Guide with Special Reference to Credit Card Frauds*, 2nd edn), Universal Law Publishing Company.

Articles and Research Papers

1. Read article *China Mounts Cyber Attacks on Indian Sites* at: <http://timesofindia.indiatimes.com/india/China-mounts-cyber-attacks-on-Indian-sites/articleshow/3010288.cms> (29 January 2010).
2. Read article *3,286 Indian Websites Hacked in Five Months* at: http://www.siliconindia.com/shownews/3286_Indian_websites_hacked_in_five_months-nid-63485.html (29 January 2010).
3. Read article *40-50 Indian Sites Hacked by Pak Cyber Criminals Monthly* at: <http://archives.infotech.indiatimes.com/articleshow/35371176.cms> (20 January 2010).
4. Read article *Pakistani Cyber criminals Deface 50 to 60 Indian Websites per day* at: <http://www.webnewswire.com/node/480067> (15 January 2010).

5. A white paper on Click Frauds can be accessed in the following links:
<http://www.hitslink.com/whitepapers/click-fraud.pdf> (24 March 2010).
Additional links on the topic of “Click Fraud” can be visited at:
<http://www.marketingtilt.com.au/what-is-click-fraud/> (23 March 2010).
<http://en.wikipedia.org/wiki/Click%5Ffraud> (24 March 2010).
<http://www.wisegeek.com/what-is-external-click-fraud.htm> (24 March 2010).
<http://www.wisegeek.com/what-is-click-fraud.htm> (24 March 2010).
<http://www.clickprotector.com/faq.asp> (24 March 2010) (FAQ on detecting and stopping Click Frauds).
http://help.yahoo.com/l/uk/yahoo/ysm/sps/faqs/acclickthru/click_fraud.html (24 March 2010).
http://www.bukisa.com/articles/186305_what-is-advertising-click-fraud (24 March 2010).
6. A paper on *Anti-Spam Laws and their Effectiveness* can be accessed at:
<http://www-users.rwth-aachen.de/guido.schryen/publications/Schryen%20-%20Anti-spam%20legislation%20-%20ICTL.pdf> (8 May 2010).

The appendices that serve as extended material for the topics addressed in this chapter are: A, B, D, E, F, J, K, L, M, O, P, Q, U, V. These are provided in the companion CD.

2 | Cyberoffenses: How Criminals Plan Them

Learning Objectives

After reading this chapter, you will be able to:

- Understand different types of cyberattacks.
 - Get an overview of the steps involved in planning cybercrime.
 - Understand tools used for gathering information about the target.
 - Get an overview on social engineering – what and how.
 - Learn about the role of cybercafes in cybercrime.
 - Understand what cyberstalking is.
 - Learn about Botnets and attack vector.
 - Get an overview on cloud computing – what and how.
-

2.1 Introduction

Technology is a “double-edged sword” as it can be used for both good and bad purposes. People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose. Computers and tools available in IT are also no exceptions; like other tool, they are used as either target of offense or means for committing an offense. In today’s world of Internet and computer networks, a criminal activity can be carried out across national borders with “false sense of anonymity”; without realizing, we seem to pass on tremendous amount of information about ourselves. Are we sure this will never be misused? Figure 2.1 gives us an idea about all those agencies that collect information about the individuals (i.e., Personally Identifiable Information such as date of birth, personal E-Mail address, bank account details and/or credit card details, etc. explained in Section 5.3.1, Chapter 5).

Chapter 1 provided an overview of *hacking, industrial espionage, network intrusions, password sniffing, computer viruses*, etc. They are the most commonly occurring crimes that target the computer. Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc. The criminals take advantage of the widespread lack of awareness about cybercrimes and cyberlaws among the people who are constantly using the IT infrastructure for official and personal purposes. People who commit cybercrimes are known as “Crackers” (Box 2.1).

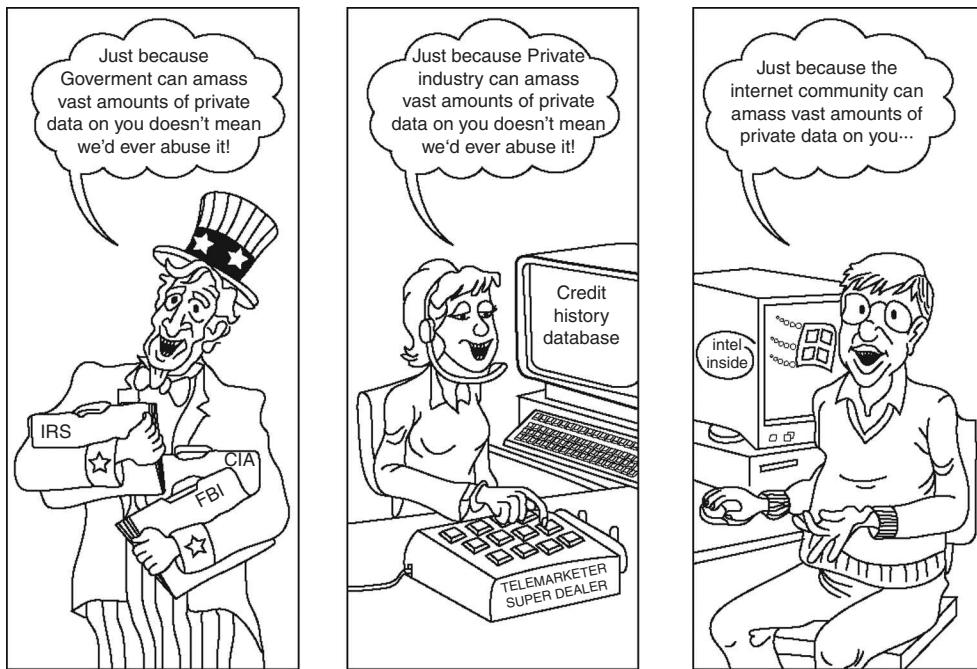


Figure 2.1 We all vouch for keeping your personal information secret!

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 29.14), Wiley India.

Box 2.1 Hackers, Crackers and Phreakers

Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who breaks into computers (refer to Box 2.2).

Brute force hacking: It is a technique used to find passwords or encryption keys. Brute force hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.

Cracker: A cracker is a person who breaks into computers. Crackers should not be confused with hackers. The term "cracker" is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.

Cracking: It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called "phreaking"). These sites usually display warnings such as "These files are illegal; we are not responsible for what you do with them."

Cracker tools: These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war dialers and worms.

Phreaking: This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.

War dialer: It is program that automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try to break in.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 11.2), Wiley India.

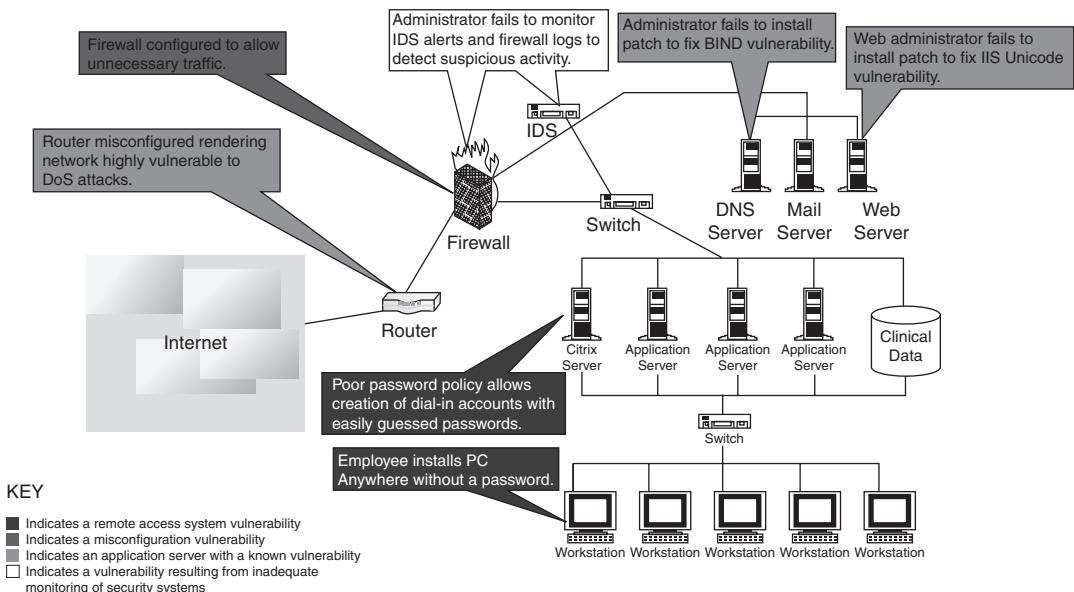


Figure 2.2 | Network vulnerabilities – sample network.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 11.6), Wiley India.

An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected. The categories of vulnerabilities that hackers typically search for are the following:

1. Inadequate border protection (border as in the sense of network periphery);
2. remote access servers (RASs) with weak access controls;
3. application servers with well-known exploits;
4. misconfigured systems and systems with default configurations.

To help the reader understand the network attack scenario, Fig. 2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.

Box 2.2 What Color is Your Hat in the Security World?

When Edward De Bono wrote his epoch making the book *The Six Thinking Hats* most successful concept that helps people to be more productive, focused, and mindfully involved, little did he know that the hats would follow suit in other domains too!! Just read on to discover about the "hats" in security world. And not only that, but also be conscious to know if any of these hats are around you to jeopardize the security of your information assets on the network.

A black hat is also called a "cracker" or "dark side hacker." Such a person is a malicious or criminal hacker. Typically, the term "cracker" is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer jargon, the meaning of "hacker" can be much broader. The name comes from the opposite of "white hat hackers."

Box 2.2 \ What Color . . . (Continued)

A white hat hacker is considered an ethical hacker. In the realm of IT, a “white hat hacker” is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. As a simplified explanation, a “white hat” generally focuses on securing IT systems, whereas a “black hat” (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

A black hat will wish to secure his/her own machine whereas a white hat might need to break into a black hat’s machine in course of an investigation. What exactly differentiates white hats and black hats is open to interpretation; however, white hats tend to cite altruistic motivations. Usually a black hat is a person who uses his knowledge of vulnerabilities and exploits for private gain, rather than revealing them either to the general public or to the manufacturer for correction. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system over which they have already obtained secure control. In the most extreme cases, black hats may work to cause damage maliciously.

Interestingly, this is not all; in the security world, there are hats of other colors too. A brown hat hacker is one who thinks before acting or committing a malice or non-malice deed. A grey hat commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 17.3), Wiley India.

2.1.1 Categories of Cybercrime

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

As explained in Section 1.5, Chapter 1, cybercrime can be targeted against individuals (persons), assets (property) and/or organizations (government, business and social).

1. **Crimes targeted at individuals:** The goal is to exploit human weakness such as greed and naivety. These crimes include financial frauds, sale of non-existent or stolen items, child pornography (explained in Section 1.5.13, Chapter 1), copyright violation, harassment, etc. with the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims. However, this also makes difficult to trace and apprehend the criminals.
2. **Crimes targeted at property:** This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive, etc.
3. **Crimes targeted at organizations:** Cyberterrorism is one of the distinct crimes against organizations/governments. Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the programs and files or plant programs to get control of the network and/or system (see Box 2.3).

Box 2.3 Patriot Hacking

Patriot hacking^[1] also known as *Digital Warfare*, is a form of vigilante computer systems' cracking done by individuals or groups (usually citizens or supports of a country) against a real or perceived threat. Traditionally, Western countries, that is, developing countries, attempts to launch attacks on their perceived enemies.

Although patriot hacking is declared as illegal in the US, however, it is reserved only for government agencies [i.e., Central Intelligence Agency (CIA) and National Security Agency (NSA)] as a legitimate form of attack and defense. Federal Bureau of Investigation (FBI) raised the concern about rise in cyberattacks like website defacements (explained in Box 1.4, Chapter 1) and denial-of-service attacks (DoS – refer to Section 4.9, Chapter 4), which adds as fuel into increase in international tension and gets mirrored it into the online world.

After the war in Iraq in 2003, it is getting popular in the North America, Western Europe and Israel. These are countries that have the greatest threat to Islamic terrorism and its aforementioned digital version.

The People's Republic of China is allegedly making attacks upon the computer networks of the US and the UK. Refer to Box 5.15 in Chapter 5.

For detailed information visit www.patriothacking.com

- 4. **Single event of cybercrime:** It is the single event from the perspective of the victim. For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.
- 5. **Series of events:** This involves attacker interacting with the victims repetitively. For example, attacker interacts with the victim on the phone and/or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault (refer to Section 2.4 on "Cyberstalking").

2.2 How Criminals Plan the Attacks

Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization. (The custodian of a property can be an individual or an organization; for discussion purpose not mentioned here.) Criminals plan passive and active attacks (see Sections 2.2.2 and 2.2.3 for more details on these topics). Active attacks are usually used to alter the system (i.e., computer network) whereas passive attacks attempt to gain information about the target. Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality.

In addition to the active and passive categories, attacks can be categorized as either inside or outside. An attack originating and/or attempted within the security perimeter of an organization is an inside attack; it is usually attempted by an "insider" who gains access to more resources than expected. An outside attack is attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

The following phases are involved in planning cybercrime:

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

2.2.1 Reconnaissance

The literal meaning of “Reconnaissance” is *an act of reconnoitering – explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy)*.

In the world of “hacking,” reconnaissance phase begins with “Footprinting” – this is the preparation toward preattack phase, and involves accumulating data about the target’s environment and computer architecture to find ways to intrude into that environment. Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities. The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are useful for launching the attack.

Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

2.2.2 Passive Attacks

A passive attack involves gathering information about a target without his/her (individual’s or company’s) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises. However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

1. Google or Yahoo search: People search to locate information about employees (see Table 2.1).
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization’s website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

Box 2.4 \ Tips for Effective Search with “Google” Search Engine

The Google search engine can be used indigenously to perform “Reconnaissance” phase of an attack. The following commands can be used effectively in the Google search engine.

http://groups.google.com: This site can be used to search the Google newsgroups.

Site: If you include [site:] in your query, Google will restrict the results to those websites in the given domain. For instance, [help site:www.google.com] will find pages about help within www.google.com. [help site:.com] will find pages about help within .com URLs (uniform resource locator). Note that, there should be no space between the “site:” and the domain. This feature is also available through advanced search page, under Advanced Web Search > Domains.

F filetype: This will search within the text of a particular type of file. The file type to search must be typed after the colon.

Link: The query [link:] will list the webpages that have links to the specified webpage. For instance, [link: www.google.com] will list webpages that have links pointing to the Google homepage. Note that there can be no space between the “link:” and the webpage URL. This functionality is also accessible from the advanced search page, under Page Specific Search > Links.

Box 2.4 Tips for . . . (Continued)

Inurl: If you include [inurl:] in your query, Google will restrict the results to documents containing that word in the URL. For instance, [inurl:google search] will return documents that mention the word "google" in their URL, and mention the word "search" anywhere in the document (URL or no). Note that there should be no space between the "inurl:" and the following word. Putting "inurl:" in front of every word in your query is equivalent to putting "allinurl:" in front of your query; this implies [inurl:google inurl:search] is the same as [allinurl: google search].

Cache: If you include other words in the query, Google will highlight those words within the cached document. For instance, [cache: www.google.com web] will show the cached content with the word "web" highlighted. This feature is also accessible by clicking on the "Cached" link on Google's main results page. The query [cache:] will show the version of the webpage that Google has in its cache. For instance, [cache: www.google.com] will show Google's cache of the Google homepage. Note that there should be no space between the "cache:" and the webpage URL.

Related: The query [related:] will list webpages that are "similar" to a specified webpage. For instance, [related: www.google.com] will list webpages that are similar to the Google homepage. Note that there should be no space between the "related:" and the webpage URL. This feature is also accessible by clicking on the "Similar Pages" link on Google's main results page, and from the advanced search page, under Page Specific Search > Similar.

Info: The query [info:] will present some information that Google has about that webpage. For instance, [info: www.google.com] will show information about the Google homepage. Note that there should be no space between the "info:" and the webpage URL. This feature is also accessible by typing the webpage URL directly into a Google search box.

Define: The query [define:] will provide a definition of the word/phrase you enter after it, gathered from various online sources. The definition will be for the entire phrase entered (i.e., it will include all the words in the exact order you typed them).

Stocks: If you begin a query with the [stocks:] operator, Google will treat the rest of the query terms as stock ticker symbols and will link to a page showing stock information for those symbols. For instance, [stocks: intc yhoo] will show information about Intel and Yahoo. (Note that you must type the ticker symbols, not the company name.) This feature is also available if you search just on the stock symbols (e.g., [intc yhoo]) and then click on the "Show stock quotes" link on the results page.

Allintitle: If you start a query with [allintitle:], Google will restrict the results to those with all of the query words in the title. For instance, [allintitle: google search] will return only documents that have both "google" and "search" in the title. This feature is also available through advanced Search page, under Advanced Web Search > Occurrences.

Intitle: If you include [intitle:] in your query, Google will restrict the results to documents containing that word in the title. For instance, [intitle:google search] will return documents that mention the word "google" in their title and the word "search" anywhere in the document (title or no). Note that there should be no space between the "intitle:" and the following word. Putting [intitle:] in front of every word in your query is equivalent to putting [allintitle:] at the front of your query; this implies that [intitle:google intitle:search] is the same as [allintitle: google search].

Allinurl: If you start a query with [allinurl:], Google will restrict the results to those with all of the query words in the URL. For instance, [allinurl: google search] will return only documents that have both "google" and "search" in the URL.

Note that [allinurl:] works on words, not on URL components. In particular, it ignores punctuation. Thus, [allinurl: foo/bar] will restrict the results to page with the words "foo" and "bar" in the URL, but won't require that they be separated by a slash within that URL, that they be adjacent, or that they be in that particular word order. There is currently no way to enforce these constraints.

Source: <http://www.google.com.tw/help/operators.html>

Network sniffing is another means of passive attack to yield useful information such as Internet Protocol (IP) address ranges, hidden servers or networks, and other available services on the system or network. The network traffic is sniffed for monitoring the traffic on the network – attacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Along with Google search, various other tools are also used for gathering information about the target/victim (Table 2.1).

Table 2.1 | Tools used during passive attacks

Name of the Tool	Brief Description	Remarks
Google Earth	Google Earth is a virtual globe, map, and geographic information program. It maps the Earth by the superimposition of images obtained from satellite imagery and provides aerial photography of the globe. It is available under three different licenses: Google Earth, a free version with limited functionality; Google Earth Plus (discontinued), with additional features; and Google Earth Pro intended for commercial use.	For more details on this tool, visit: http://earth.google.com/ Like “Google Earth,” similar details can be obtained from http://www.wikimapia.org/ Indian Space Research Organization (ISRO) unveiled its beta version of Bhuvan (meaning Earth in Sanskrit), a Web-based tool like Google Earth, that promises better 3-D satellite imagery of India than is currently being offered by Google Earth and that too with India-specific features such as weather information and even administrative boundaries of all states and districts, visit: http://bhuvan.nrsc.gov.in/
Internet Archive	The Internet Archive is an Internet library, with the purpose of offering permanent access for researchers, historians and scholars to historical collections that exist in digital format. It includes texts, audio, moving images, and software as well as archived webpages in our collections.	An attacker gets the information about latest update made to the target’s website as well as can dig the information which maybe available in the history (e.g., contact list of executives and higher management officials are always updated). For more details on this tool, visit: http://www.archive.org/index.php
Professional Community	LinkedIn is an interconnected network of experienced professionals from around the world, representing 170 industries and 200 countries.	One can find details about qualified professionals. For more details on this tool, visit: http://www.linkedin.com/
People Search	People Search provides details about personal information: date of birth, residential address, contact number, etc.	To name a few, visit: <ul style="list-style-type: none"> • http://www.whitepagesinc.com • http://www.intelius.com/ • http://www.whitepages.com/
Domain Name Confirmation	To perform searches for domain names (e.g., website names) using multiple keywords. This helps to enable to find every registered domain name in “com,” “net,” “org,” “edu,” “biz,” etc.	For more details on this tool, visit: <ul style="list-style-type: none"> • http://www.namedropplers.com/ • http://www.binarypool.com/bytes.html

(Continued)

Table 2.1 | (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
WHOIS	<p>This is a domain registration lookup tool. This utility is used for communicating with WHOIS servers located around the world to obtain domain registration information.</p> <p>WHOIS supports IP address queries and automatically selects the appropriate WHOIS server for IP addresses. This tool will lookup information on a domain, IP address, or a domain registration information. You can select a specific WHOIS server, or you can use the “Default” option which will select a server for you.</p>	<p>For more details on this tool, visit:</p> <ul style="list-style-type: none"> • http://whois.domaintools.com/ • http://www.whois.net/ • http://www.samspade.org/ <p>For further details of this lookup utility, visit:</p> <ul style="list-style-type: none"> • http://resellers.tucows.com/openrsr/whois/ • http://www.nsaudit.com/docs/html/tools/Whois.htm
Nslookup	The name nslookup means “name server lookup.” The tool is used on Windows and Unix to query domain name system (DNS) servers to find DNS details, including IP addresses of a particular computer and other technical details such as mail exchanger (MX) records for a domain and name server (NS) servers of a domain.	<p>For more details on this tool, visit:</p> <ul style="list-style-type: none"> • http://www.kloth.net/services/nslookup.php • http://nslookup.downloadsoftware4free.com/
Dnsstuff	Using this tool, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookup, WHOIS lookups, etc.	<p>For more details on this tool, visit: http://www.dnsstuff.com/</p>
Traceroute	This is the best tool to find the route (i.e., computer network path) to a target system. It determines the route taken by packets across an IP network.	<p>For more details on this tool, visit: http://www.rjsmith.com/traceroute.html</p>
VisualRoute Trace	This is a graphical tool which determines where and how virtual traffic on the computer network is flowing between source and target destination.	<p>For more details on this tool, visit: http://www.visualware.com/</p>
eMailTrackerPro	eMailTrackerPro analyzes the E-Mail header and provides the IP address of the system that sent the mail.	<p>For more details on this tool, visit: http://www.emailtrackerpro.com/</p>
HTTrack	This tool acts like an offline browser. It can mirror the entire website to a desktop. One can analyze the entire website by being offline.	<p>For more details on this tool, visit: http://www.httrack.com/</p>
Website Watcher	The tool can be used to keep the track of favorite websites for an update. When the website undergoes an update/change, this tool automatically detects it and saves the last two versions onto the desktop.	<p>For more details on this tool, visit: http://www.aignes.com/</p>
Competitive Intelligence	Competitive intelligence can provide information related to almost any product, information on recent industry trends, or information about geopolitical indications. Effective use of competitive intelligence can reveal attack against the website or an industrial espionage.	<p>To name a few, visit:</p> <ul style="list-style-type: none"> • http://digital.com/ • http://www.amity.edu/aici/

Note: IP is Internet Protocol here.

2.2.3 Active Attacks

An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase. It involves the risk of detection and is also called “*Rattling the doorknobs*” or “*Active reconnaissance*.”

Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

Table 2.2 gives the list of tools used for active attacks – some of the tools are also used during “vulnerability assessment” and/or “penetration testing.” Refer to Appendix E in CD.

Table 2.2 | Tools used during active attacks

Name of the Tool	Brief Description	Remarks
Arphound	This is a tool that listens to all traffic on an Ethernet network interface. It reports IP/media access control (MAC) address pairs as well as events, such as IP conflicts, IP changes and IP addresses with no reverse DNS, various Address Resolution Protocol (ARP) Spoofing and packets not using the expected gateway.	This is open-source software. For more details on this tool and download, visit: http://www.nottale.net/index.php?project=arphound
Arping	This is a network tool that broadcasts ARP packets and receives replies similar to “ping.” It is good for mapping a local network and finding used IP space. It broadcasts a “who-has ARP packet” on the network and prints answers. It is very useful when trying to pick an unused IP for a Net to which routing does not exist as yet.	This is open-source software. For more details on this tool and download, visit: http://www.habets.pp.se/synscan/programs.php?prog=arping
Bing	This is used for Bandwidth Ping. It is a point-to-point bandwidth measurement tool based on ping. It can measure raw throughput between any two network links. Bing determines the real (raw as opposed to available or average) throughput on a link by measuring Internet Control Message Protocol (ICMP) echo requests roundtrip times for different packet sizes for each end of the link.	This is open-source software. For installation and usage information, visit: http://ai3.asti.dost.gov.ph/sat/bing.html
Bugtraq	This is a database of known vulnerabilities and exploits providing a large quantity of technical information and resources.	This software is for free usage. Visit the following site for more details: http://www.securityfocus.com/bid
Dig	This is used to perform detailed queries about DNS records and zones, extracting configuration, and administrative information about a network or domain.	This is open-source software. For additional technical details, visit: http://www.isc.org/index.pl?sw/bind/
DNStracer	This is a tool to determine the data source for a given DNS server and follow the chain of DNS servers back to the authoritative sources.	This is also open-source software. For additional technical details, visit: http://www.mavetju.org/unix/dnstracer.php

(Continued)

Table 2.2 | (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
Dsniff	This is a network auditing tool to capture username, password, and authentication information on a local subnet.	This is open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
Filesnarf	This is a network auditing tool to capture file transfers and file sharing traffic on a local subnet.	This is also open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
FindSMB	This is used to find and describe server message block (SMB) servers on the local network.	It is open-source software; visit the following site for downloads: http://us3.samba.org/samba/
Fping	This is a utility similar to ping used to perform parallel network discovery.	For this open-source software, visit: http://www.fping.com/
Fragroute	This intercepts, modifies and rewrites egress traffic destined for a specified host, implementing several intrusion detection system (IDS) evasion techniques.	This is another open-source material; visit: http://www.monkey.org/~dugsong/fragroute/
Fragtest	This tests the IP fragment reassembly behavior of the Transmission Control Protocol (TCP) stack on a target. It intercepts, modifies and rewrites egress traffic destined for a specified host, implementing most of the attacks.	For more details on this open-source software, visit: http://www.monkey.org/~dugsong/fragroute/
Hackbot	This is a host exploration tool, simple vulnerability scanner and banner logger.	Another open-source software, whose details can be found at: http://freshmeat.net/projects/hackbot/
Hmap	This is used to obtain detailed fingerprinting of web servers to identify vendor, version, patch level, including modules and much more. <i>Hmap</i> is a web server fingerprinting tool.	Details of this open-source software can be found at: http://ujeni.murkyroc.com/hmap/
Hping	This is a TCP/IP packet assembler and analyzer. It can perform firewall ruleset testing, port scanning, network type of service/quality-of-service (TOS/QOS) testing, maximum transmission unit (MTU) discovery, alternate-protocol traceroute, TCP stack auditing, and much more. Using <i>hping</i> you can do the following: <ul style="list-style-type: none"> • Firewall testing; • advanced port scanning; • network testing, using different protocols, TOS, fragmentation; • manual path MTU discovery; • advanced traceroute, under all the supported protocols; • remote OS fingerprinting; • remote uptime guessing; • TCP/IP stacks auditing; • hping can also be useful to students that are learning TCP/IP. 	This is open-source software. For additional technical details, visit: http://www.hping.org/

(Continued)

Table 2.2 | (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
Hping	Hping works on the following Unix-like systems: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.	
Httping	This is similar to “ping,” that is, hping, but for HTTP requests. It shows how long a URL will take to connect, send a request, and receive a reply.	This is open-source software. For additional technical details, visit: http://www.vanheusden.com/httping/
Hunt	This is a tool for exploiting well-known weaknesses in the TCP/IP protocol suite.	This is also open-source software. For additional technical details, visit: http://lin.fsid.cvut.cz/~kra/index.html
Libwhisker	This is an application library designed to assist in scannabilities.	Details of this open-source software can be found at: http://www.wiretrip.net/rfp/lw.asp
Mailsnarf	This is a network auditing tool to capture SMTing for CGI/web vulnerP and POP3 E-Mail traffic (including message headers, bodies, and attachments) on a local subnet.	For this open-source software, you can visit: http://monkey.org/~dugsong/dsniff/
Msgsnarf	This is a network auditing tool to capture instant message (Yahoo, MSN, ICQ, iChat, AIM, and many more) traffic on a local subnet.	Same as above
NBTScan	This is a utility for scanning networks for NetBIOS information. It reports IP address, NetBIOS name, logged-in username, and MAC address.	Details of this open-source material can be found at: http://www.inetcat.org/software/nbtscan.html
Nessus	This is a powerful, fast, and modular security scanner that tests for many thousands of vulnerabilities. ControlScans’ system can also be used to create custom Nessus reports.	To know more about this open-source utility, visit: http://www.nessus.org/
Netcat	This is a utility to read and write custom TCP/ User Datagram Protocol (UDP) data packets across a network connection for network debugging or exploration.	Explore more details of this open-source utility at: http://www.atstake.com/research/tools/network_utilities/
Nikto	This is a web server vulnerability scanner that tests over 2,600 potentially dangerous files/CGIs on over 625 types of servers. This tool also performs comprehensive tests against web servers for multiple items and version-specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).	Nikto is an open-source web server scanner; visit the following site for more detail: http://www.cirt.net/code/nikto.shtml
Nmap	This is a port scanner, operating system fingerprinter, service/version identifier, and much more. Nmap is designed to rapidly scan large networks.	For details of this open-source software, visit: http://insecure.org/nmap/

(Continued)

Table 2.2 | (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
Pathchar	This is a network tool for inferring the characteristics of Internet paths, including Layer 3 hops, bandwidth capacity, and autonomous system information.	For further details, visit: http://ee.lbl.gov/
Ping	This is a standard network utility to send ICMP packets to a target host.	For further details, visit: http://www.controlscan.com/auditingtools.html#
ScanSSH	<p>This supports scanning a list of addresses and networks for open proxies, SSH Protocol servers, and Web and SMTP servers. Where possible, it displays the version number of the running services.</p> <p>ScanSSH supports the following features:</p> <ul style="list-style-type: none"> • Variable scanning speed: per default, ScanSSH sends out 100 probes per second; • open proxy detection; • random sampling: it is possible to randomly sample hosts on the Internet. 	<p>The first version of the ScanSSH Protocol scanner was released in September 2000.</p> <p>For further details and downloading the current version, visit: http://www.monkey.org/~provos/scanssh/</p>
SMBclient	<p>This helps a client to talk to an SMB (Samba, Windows File Sharing) server. Operations include getting files from the server, putting files on the server, retrieving directory information, and much more.</p> <p>It is an open-source/free software suite that has, since 1992, provided file and print services to all types of SMB/common Internet file system (CIFS) clients, including the numerous versions of Microsoft Windows operating systems. Samba is freely available under the GNU General Public License.</p>	
SMTPscan	This is a tool to determine the type and version of a remote Simple Mail Transfer Protocol (SMTP) mail server based on active probing and analyzing error codes of the target SMTP server.	For further details, visit: http://www.greyhats.org/outils/smtpscan/
TCPdump	It is a network tool for the protocol packet capture and dumper program.	For further details, visit: http://ee.lbl.gov/
TCPreplay	<p>This is a utility to read captured TCPdump/pcap data and “replay” it back onto the network at arbitrary speeds.</p> <p>TCPReplay is a suite of licensed tools written by Aaron Turner for Unix operating systems. It gives you the ability to use previously captured traffic to test a variety of network devices. It allows you to classify traffic as client or server; rewrite open system interconnection (OSI) Layers 2, 3 and 4 headers; and finally replay the traffic back onto the network and through other</p>	<p>TCPReplay suite includes the following tools:</p> <ul style="list-style-type: none"> • TCPprep: It is a multi-pass packet capture (pcap) file preprocessor which determines packets as client or server and creates cache files used by TCPReplay and TCPrewrite. • TCPrewrite: It is a pcap file editor which rewrites TCP/IP and Layer 2 packet headers.

(Continued)

Table 2.2 | (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
	<p>devices such as switches, routers, firewalls, network-based intrusion detection system (NIDS), and intrusion prevention system (IPS).</p> <p>TCPReplay supports both single and dual NIC modes for testing both sniffing and inline devices.</p> <p>TCPReplay is used by numerous firewalls, IDS, IPS, and other networking vendors, enterprises, universities, laboratories, and open-source projects.</p>	<ul style="list-style-type: none"> • TCPReplay: It replays pcap files at arbitrary speeds onto the network. • TCPReplay-edit: It replays and edits pcap files at arbitrary speeds onto the network. • TCPbridge: It bridges two network segments with the power of TCPrewrite. <p>For further details, visit: http://tcpreplay.synfin.net/trac/</p>
THC-Amap	This is a scanner to remotely fingerprint and identify network applications and services.	<p>For further details, visit: http://freeworld.thc.org/releases.php</p>
Traceroute	This is a standard network utility to trace the logical path to a target host by sending ICMP or UDP packets with incrementing tunneled transport layer security (TTLs).	<p>For further details, visit: http://ee.lbl.gov/</p>
URLsnarf	This is a network auditing tool to capture HTTP traffic on a local subnet.	<p>For further details, visit: http://monkey.org/~dugsong/dsniff/</p>
XProbe2	This is a tool employing several techniques to actively fingerprint the operating system of a target host.	<p>For further details, visit: http://www.sys-security.com/html/projects/X.html</p>

Note: IP is Internet Protocol here.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Table 35.2), Wiley India.

2.2.4 Scanning and Scrutinizing Gathered Information

Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:

1. **Port scanning:** Identify open/close ports and services. Refer to Box 2.5.
2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

Box 2.5 Ports and Ports Scanning

A port is an interface on a computer to which one can connect a device. TCP/IP Protocol suite made out of the two protocols, TCP and UDP, is used universally to communicate on the Internet. Each of these has ports 0 through 65536 (i.e., the range is from 2^0 to 2^{16} for binary address calculation). The port numbers are divided into three ranges:

Box 2.5 Ports and Ports . . . (Continued)

1. Well-known ports (from 0 to 1023);
2. registered ports;
3. dynamic and/or private ports.

The list of well-known port numbers and short description about the services offered by each of these are provided in Table 2.3.

Table 2.3 | Well-known port numbers

Port Number	Port Description	Port Number	Port Description
1	TCP port service multiplexer (TCPMUX)	118	Structured query language (SQL) services
5	Remote job entry (RJE)	119	NNTP (Newsgroup)
7	ECHO	137	NetBIOS name service
18	Message Send Protocol (MSP)	139	NetBIOS datagram service
20	FTP – Data	143	Internet Message Access Protocol (IMAP)
21	FTP – Control	150	NetBIOS session service
22	Secure shell (SSH) remote log-in protocol	156	SQL server
23	Telnet	161	Simple Network Management Protocol (SNMP)
25	Simple Mail Transfer Protocol (SMTP)	179	Border Gateway Protocol (BGP)
29	MSG ICP	190	Gateway Access Control Protocol (GACP)
37	Time	194	Internet relay chat (IRC)
42	Nameserv (host name server)	197	Directory location service (DLS)
43	WHOIS	389	Lightweight Directory Access Protocol (LDAP)
49	Log-in (log-in host protocol)	396	Novell netware over IP
53	Domain name system (DNS)	443	Secure Hypertext Transfer Protocol (S-HTTP)
69	Trivial File Transfer Protocol (TFTP)	444	Simple Network Paging Protocol (SNPP)
70	Gopher services	445	Microsoft-DS
79	Finger	458	Apple quick time
80	HTTP	546	DHCP client
103	X.400 Standard	547	DHCP server
108	SNA gateway access server	563	SNEWS
109	POP2	569	MSN
110	POP3	1080	Socks
115	Simple File Transfer Protocol (SFTP)		

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Chapter 35, p. 774), Wiley India.

Box 2.5 \ Ports and Ports . . . (*Continued*)

There are some well-known IP ports (0–999) that require scanning owing to vulnerabilities known about them. In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are preassigned to them by the Internet Assigned Numbers Authority (IANA), an organization working under the auspices of the Internet Architecture Board (IAB), responsible for assigning new Internet-wide IP addresses.

Table 2.3 lists the well-known ports along with the services run on them. Although public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws, and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Port Scanning

A “port” is a place where information goes into and out of a computer and so, with port scanning, one can identify open doors to a computer. Ports are basically entry/exit points that any computer has, to be able to communicate with external machines. Each computer is enabled with three or more external ports. These are the ports used by the computer to communicate with the other computers, printer, modem, mouse, video game, scanner, and other peripherals. The important characteristic about these “external ports” is that they are indeed external and visible to the naked eye. Port scanning is often one of the first things an attacker will do when attempting to penetrate a particular computer. Tools such as Nmap (Table 2.2 lists a few vulnerability assessment tools) offer an automated mechanism for an attacker to not only scan the system to find out what ports are “open” (meaning being used), but also help to identify what operating system (OS) is being used by the system.

Port scanning is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked. Port scanning is an act of systematically scanning a computer’s ports. In technological terms, “port scanning” refers to the act of using various open-ended technologies, tools, and commands to be able to communicate with another remote computer system or network, in a stealth mode, without being apparent, and be able to obtain certain sensitive information about the functions of system and the properties of the hardware and the software being used by the remote systems.

In “portscan,” a host scans for listening ports on a single target host. In “portsweep,” a host scans multiple hosts for a specific listening port. The result of a scan on a port is usually generalized into one of the following three categories:

1. **Open or accepted:** The host sent a reply indicating that a service is listening on the port.
2. **Closed or not listening:** The host sent a reply indicating that connections will be denied to the port.
3. **Filtered or blocked:** There was no reply from the host.

TCP/IP suite of protocols is used to communicate with other computers for specific message formats. Most of these protocols are tied to specific port numbers that are used to transfer particular message formats as data. Security administrators as well as attackers have a special eye on few well-known ports and protocols associated with it.

1. Ports 20 and 21 – File Transfer Protocol (FTP) – are used for uploading and downloading of information.
2. Port 25 – Simple Mail Transfer Protocol (SMTP) – is used for sending/receiving E-Mails.
3. Port 23 – Telnet Protocol – is used to connect directly to a remote host and Internet control message.
4. Port 80 – It is used for Hypertext Transfer Protocol (HTTP).
5. Internet Control Message Protocol (ICMP) – It does not have a port abstraction and is used for checking network errors, for example, ping.

Box 2.5 Ports and Ports . . . (Continued)

Open ports present two vulnerabilities of which administrators must be wary:

1. Vulnerabilities associated with the program that is delivering the service.
2. Vulnerabilities associated with the OS that is running on the host.

Closed ports present only the latter of the two vulnerabilities that open ports do. Blocked ports do not present any reasonable vulnerabilities. There is also the possibility that there are no known vulnerabilities in either the software (program) or the OS at the given time.^[2]

The scrutinizing phase is always called “enumeration” in the hacking world. The objective behind this step is to identify:

1. The valid user accounts or groups;
2. network resources and/or shared resources;
3. OS and different applications that are running on the OS.

Most of the tools listed in Table 2.2 are used for computer network scanning as well.



Usually, most of the attackers consume 90% of the time in scanning, scrutinizing and gathering information on a target and 10% of the time in launching the attack.

2.2.5 Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password (we will address it in Chapter 4);
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

2.3 Social Engineering

Social engineering is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action. Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes. It is generally agreed that people are the weak link in security and this principle makes social engineering possible. A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.

Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. Social engineer studies the human behavior so that

Box 2.6 Social Engineering Example

Mr. Joshi: Hello?

The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user's home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.

Mr. Joshi: Ohh ... okay. I will be at my home by then, anyway.

Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?

Mr. Joshi: Username is "pjoshi." None of my files will be lost in the move, right?

Caller: No sir. But we will have to check your account to ensure the same. What is the password of that account?

Mr. Joshi: My password is "ABCD1965," all characters in upper case.

Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there.

Mr. Joshi: Thank you. Bye.

Caller: Bye and have a nice day.

people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble. The sign of truly successful social engineers is that they receive information without any suspicion. A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on (see Box 2.6).

2.3.1 Classification of Social Engineering

Human-Based Social Engineering

Human-based social engineering refers to person-to-person interaction to get the required/desired information. An example is calling the help desk and trying to find out a password.

1. **Impersonating an employee or valid user:** "Impersonation" (e.g., posing oneself as an employee of the same organization) is perhaps the greatest technique used by social engineers to deceive people. Social engineers "take advantage" of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his/her badge, etc., or pretending to be an employee or valid user on the system.
2. **Posing as an important user:** The attacker pretends to be an important user – for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system. The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.
3. **Using a third person:** An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.
4. **Calling technical support:** Calling the technical support for assistance is a classic social engineering example. Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

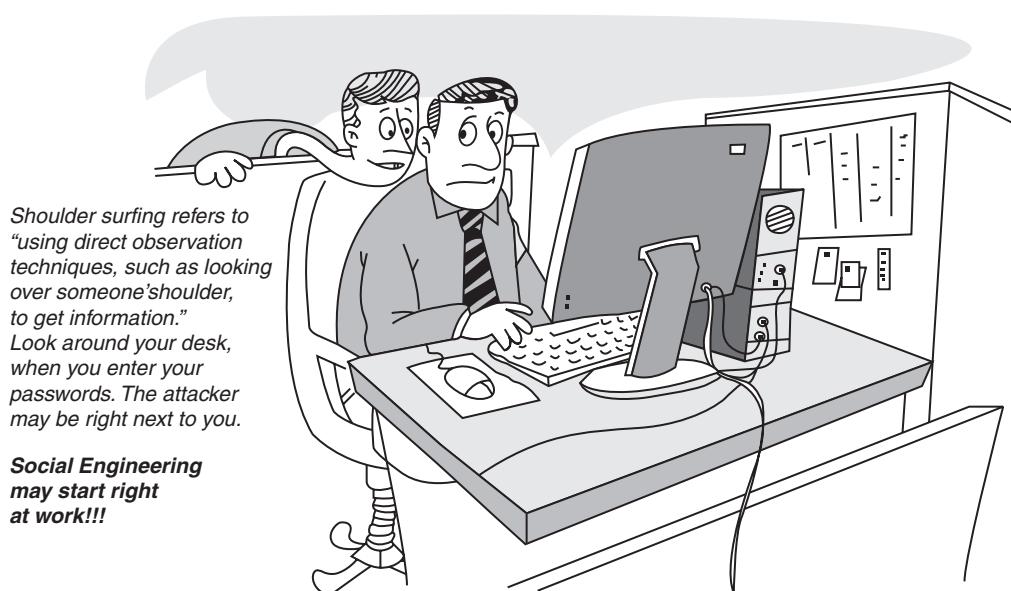


Figure 2.3 | Social engineering – shoulder surfing.

5. **Shoulder surfing:** It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system (Fig. 2.3).
6. **Dumpster diving:** It involves looking in the trash for information written on pieces of paper or computer printouts. This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded. It is also called dumpstering, binning, trashing, garbing or garbage gleaning. “Scavenging” is another term to describe these habits. In the UK, the practice is referred to as “binning” or “skipping” and the person doing it is a “binner” or a “skipper.”

In practice, *dumpstering* is more like fishing around than diving in. Usually, people dumpster dive to search the items, to reclaim those, which have been disposed of but can still be put to further use, for example, E-Waste, furniture, clothes, etc. The term “dumpster diving” may have originated from the notional image of someone leaping into large rubbish bins, the best known of which are produced under the name “dumpster.” “Scavenging” is equivalent of “dumpster diving,” in the digital world. It is a form in which discarded articles and information are scavenged in an attempt to obtain/recover advantageous data, if it is possible to do so. Consider, for example, going through someone's trash to recover documentation of his/her critical data [e.g., social security number (SSN) in the US, PAN number in India, credit card identity (ID) numbers, etc.]. According to a definition in the glossary of terms for the convoluted terminology of information warfare, “scavenging” means “searching through object residue (e.g., discarded disks, tapes, or paper) to acquire sensitive data without authorization.”

Computer-Based Social Engineering

Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet. For example, sending a fake E-Mail to the user and asking him/her to re-enter a password in a webpage to confirm it.

1. **Fake E-Mails:** The attacker sends fake E-Mails (see Box 2.7) to numerous users in such that the user finds it as a legitimate mail. This activity is also called “Phishing” (we shall address it in Chapter 5). It is an attempt to entice the Internet users (netizens) to reveal their sensitive personal information, such as user-names, passwords and credit card details by impersonating as a trustworthy and legitimate organization and/or an individual. Banks, financial institutes and payment gateways are the common targets. Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website. Thus, Phishing is also an example of social engineering techniques used to fool netizens. The term “Phishing” has been evolved from the analogy that Internet scammers are using E-Mails lures to *fish* for passwords and financial data from the sea of Internet users (i.e., netizens). The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users. As hackers have a tendency of replacing “f” with “ph,” the term “Phishing” came into being.

Box 2.7 Fake E-Mails

Free websites are available to send fake E-Mails. From Fig. 2.4, one can notice that “To” in the text box is a blank space. Hence, anyone can fill any E-Mail address with the intention of fooling the receiver of the E-Mail. In such a case when the receiver will read the mail, he/she would think that the E-Mail has been received from a legitimate sender.



Figure 2.4 | Sending fake E-Mails.

Source: <http://deadfake.com/Send.aspx> (2 April 2009).

2. **E-Mail attachments:** E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed. Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment. We will address keylogger, viruses, Trojans, and worms in Chapter 4.
3. **Pop-up windows:** Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

Social engineering indeed is a serious concern as revealed by the following past statistics on numbers:

1. As per Microsoft Corporation recent (October 2007) research, there is an increase in the number of security attacks designed to steal personal information (PI) or the instances of tricking people to provide it through social engineering. According to an FBI survey, on average 41% of security-related losses are the direct result of employees stealing information from their companies. The average cost per internal incident was US\$ 1.8 million.
2. The Federal Trade Commission (FTC) report of 2005 shows that “more than one million consumer fraud and ID theft complaints have been filed with federal, state, and local law enforcement agencies and private organizations” (2005, Consumer Fraud and Identity Theft section, para 1; we will discuss ID Theft in Chapter 5).
3. According to a 2003 survey [released on 2 April 2006 by the United States Department of Justice (Identity Theft Hits Three Percent, para 1)], “An estimated 3.6 million – or 3.1% – of American households became victims of ID theft in 2004.” This means that now, more than ever, individuals are at a high risk of having their PI stolen and used by criminals for their own personal gain.

Typically, many organizations have information valuable enough to justify expensive protection mechanisms/security mechanisms. Critical information may include patient records in the medical and healthcare domain [known as protected health information (PHI)], corporate financial data, electronic funds transfers, access to financial assets in the financial services domain, and PI about clients or employees. Compromising critical information can have serious consequences, including the loss of customers, criminal actions being brought against corporate executives, civil law cases against the organization, loss of funds, loss of trust in the organization, and collapse of the organization. To respond to the threats, organizations implement InfoSec plans to establish control of information assets. However, “social engineers” try to device a way to work their way around this to obtain the valuable information, an illicit act on ethical grounds.

Social engineering succeeds by exploiting the trust of the victim. Hence, continuous training/awareness sessions about such attacks are one of the effective countermeasures. Strict policies about service desk staff never asking for personally identifying information, such as username and passwords, over the phone or in person can also educate potential victims and recognize a social engineering attempt.



Social engineering and dumpster diving are also considered passive information-gathering methods.

2.4 Cyberstalking

The dictionary meaning of “stalking” is an “*act or process of following prey stealthily – trying to approach somebody or something*.” Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group

of individuals, or organization. The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.^[3]

Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person. It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

2.4.1 Types of Stalkers

There are primarily two types of stalkers.

1. **Online stalkers:** They aim to start the interaction with the victim directly with the help of the Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.
2. **Offline stalkers:** The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet (see Table 2.1). The victim is not aware that the Internet has been used to perpetuate an attack against them.

2.4.2 Cases Reported on Cyberstalking

The majority of cyberstalkers are men and the majority of their victims are women. Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking. In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbor. However, there also have been many instances of cyberstalking by strangers.

2.4.3 How Stalking Works?

It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

Box 2.8 Cyberbullying

The National Crime Prevention Council defines Cyberbullying as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."

www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defines cyberbullying as "a situation when a child, tween, or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology."

The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults.^[4]

Source: <http://en.wikipedia.org/wiki/Cyber-bullying> (2 April 2009).

5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails (refer to Chapter 5).

2.4.4 Real-Life Incident of Cyberstalking

Case Study

The Indian police have registered first case of cyberstalking in Delhi^[5] – the brief account of the case has been mentioned here. To maintain confidentiality and privacy of the entities involved, we have changed their names.

Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad. The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.

A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days. This person was chatting on the Internet, using her name and giving her address, talking in obscene language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.

This was the first time when a case of cyberstalking was registered. Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

2.5 Cybercafe and Cybercrimes

In February 2009, Nielsen survey^[6] on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students. Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.

In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or false terrorist communication. Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes. Cybercafes have also been used regularly for sending obscene mails to harass people.

Public computers, usually referred to the systems, available in cybercafes, hold two types of risks. First, we do not know what programs are installed on the computer – that is, risk of malicious programs such as *keyloggers* or *Spyware*, (we will discuss it in Chapter 4) which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior. Second, over-the-shoulder peeping (i.e., shoulder surfing) can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.

Indian Information Technology Act (ITA) 2000^[7] (it is discussed in great detail in Chapter 6) does not define cybercafes and interprets cybercafes as “network service providers” referred to under the erstwhile Section 79, which imposed on them a responsibility for “due diligence” failing which they would be liable for the offenses committed in their network. The concept of “due diligence” was interpreted from the various provisions in cyber-cafe regulations where available or normal responsibilities were expected from network service providers.

Cybercriminals prefer cybercafes to carry out their activities. The criminals tend to identify one particular personal computer (PC) to prepare it for their use. Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target – techniques used for this are discussed in Chapter 4. Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

A recent survey conducted in one of the metropolitan cities in India reveals the following facts (this is an eye-opener after going through the following observations:

1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
3. Several cybercafes had installed the software called “Deep Freeze” for protecting the computers from prospective malware attacks. Although such intent is noble, this software happens to help cybercriminals hoodwink the investigating agencies. Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the “restart” button.^[8] Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Interet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack (Phishing attacks are explained in Chapter 5) was carried out, to retrieve logged files.
4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down. Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.
5. Pornographic websites and other similar websites with indecent contents are not blocked.
6. Cybercafe owners have very less awareness about IT Security and IT Governance.
7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.
8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes – one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR). Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security.

There are thousands of cybercafes across India. In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe.



There is an expectation that the Indian Computer Emergency Team referred to under Section 70B of ITA 2008 may itself be designated as the agency of the Central Government with a national jurisdiction and (Computer Emergency Response Team) CERT, and may itself be stepping into the shoes of the Indian Computer Emergency Team.^[7,8]

Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout:** While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click “logout” or “sign out” before leaving the system. Simply closing the browser window is not enough, because if somebody uses the same service after you then one can get an easy access to your account. However, do not save your login information through options that allow automatic login. Disable such options before logon.
2. **Stay with the computer:** While surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.
3. **Clear history and temporary files:** Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files. Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used. Therefore, before you begin browsing, do the following in case of the browser Internet Explorer:
 - Go to *Tools* → *Internet options* → click the *Content* tab → click *AutoComplete*. If the checkboxes for passwords are selected, deselect them. Click *OK* twice.
 - After you have finished browsing, you should clear the history and temporary Internet files folders. For this, go to *Tools* → *Internet options* again → click the *General* tab → go to *Temporary Internet Files* → click *Delete Files* and then click *Delete Cookies*.
 - Then, under history, click clear history. Wait for the process to finish before leaving the computer.
4. **Be alert:** One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.
5. **Avoid online financial transactions:** Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details. In case of urgency one has to do it; however, one should take the precaution of changing all the passwords as soon as possible. One should change the passwords using a more trusted computer, such as at home and/or in office.
6. **Change passwords:** The screenshot displayed in Fig. 2.5 by ICICI Bank about changing the bank account/transaction passwords is the best practice to be followed.^[9]
7. **Virtual keyboard:** Nowadays almost every bank has provided the virtual keyboard on their website. The advantages of utilizing virtual keyboard and its functions are displayed in the screenshot shown in Fig. 2.6.^[10]
8. **Security warnings:** One should take utmost care while accessing the websites of any banks/financial institution. The screenshot in Fig. 2.7 displays security warnings very clearly (marked in bold rectangle), and should be followed while accessing these financial accounts from cybercafe.

The screenshot shows the ICICI Bank homepage with a sidebar on the left containing links for Secure Banking, Secure Yourself While..., Learn More, and Contact US. The main content area features a section titled "Cyber Cafe Security" with text about changing passwords after using a shared computer. To the right is a sidebar with links for About Us, Careers, Site Map, Login, Forgot Password, New User, and Online Security.

Figure 2.5 | Cybercafe security.

Source: <http://www.icicibank.com/pfsuser/temp/cybersec.htm> (27 June 2009).

The screenshot shows the "Virtual Keyboard" application interface. It includes a physical keyboard layout at the top, a virtual keyboard grid below it, and a text input field. The main content area has a header "Virtual Keyboard for Internet Banking" and sections for "Advantage of a Virtual Keyboard" and "Process To Use Virtual Keyboard". It also includes a list of key functions and definitions for Caps Lock, Back Space, Clear, and Tab.

Figure 2.6 | Virtual keyboard.

Source: <http://www.icicibank.com/pfsuser/webnews/virtualkeyboard.htm> (27 June 2009).

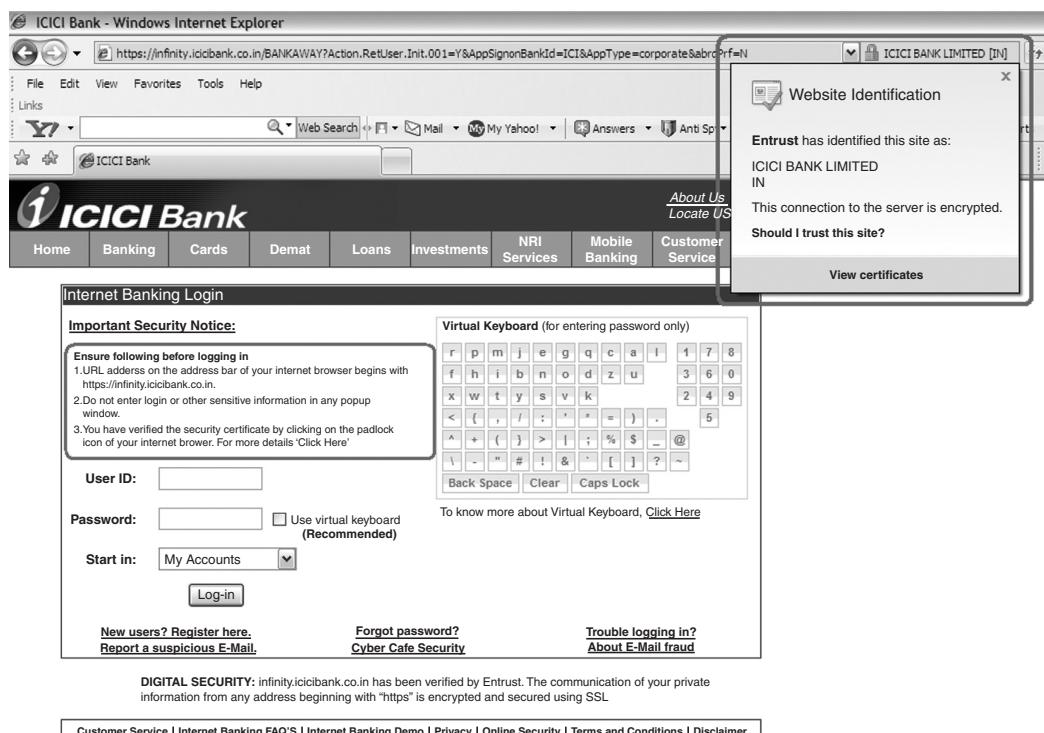


Figure 2.7 | Security warnings.

Source: <http://www.icicibank.com/pfsuser/webnews/virtualkeybord.htm> (27 June 2009).

Individual should take care while accessing computers in public places, that is, accessing the Internet in public places such as hotels, libraries and holiday resorts. Moreover, one should not forget that whatever is applicable for cybercafes (i.e., from information security perspective) is also true in the case of all other public places where the Internet is made available (refer to Appendix J in CD). Hence, one should follow all tips about safety and security while operating the systems from these facilities.

2.6 Botnets: The Fuel for Cybercrime

2.6.1 Botnet

The dictionary meaning of Bot is “(*computing*) an automated program for doing some particular task, often over a network.”

Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically. The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.^[11]

In simple terms, a Bot is simply an automated computer program (explained in Box 1.2, Chapter 1). One can gain the control of your computer by infecting them with a virus or other Malicious Code that gives the access. Your computer system maybe a part of a Botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks (the term is discussed in detail in Chapter 4).

A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge. "Zombie networks" (explained in Chapter 1, Fig. 1.3) have become a source of income for entire groups of cybercriminals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.

If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums. Obfuscation and encryption of these programs' code can also be ordered in the same way to protect them from detection by antivirus tools. Another option is to steal an existing Botnet. Figure 2.8 explains how Botnets create business.

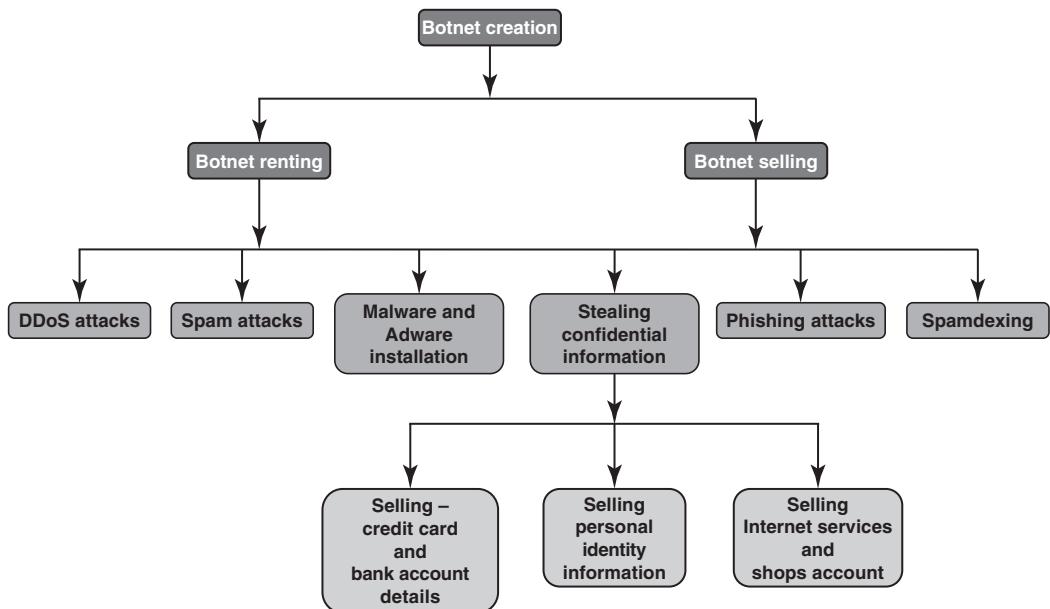


Figure 2.8 | Botnets are used for gainful purposes.

Box 2.9 Explanation for Technical Terms used in Fig. 2.8

Malware: It is malicious software, designed to damage a computer system without the owner's informed consent. Viruses and worms are the examples of malware.

Adware: It is advertising-supported software, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.

Spam: It means unsolicited or undesired E-Mail messages (this is discussed in detail in Chapter 5).

Spamdexing: It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.

DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods (this is discussed in details in Chapter 4).

One can reduce the chances of becoming part of a Bot by limiting access into the system. Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open. One can ensure following to secure the system: [12,13]

1. **Use antivirus and anti-Spyware software and keep it up-to-date:** It is important to remove and/or quarantine the viruses. The settings of these softwares should be done during the installations so that these softwares get updated automatically on a daily basis.
2. **Set the OS to download and install security patches automatically:** OS companies issue the security patches for flaws that are found in these systems.
3. **Use a firewall to protect the system from hacking attacks while it is connected on the Internet:** A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. A firewall is different from antivirus protection. Antivirus software scans incoming communications and files for troublesome viruses vis-à-vis properly configured firewall that helps to block all incoming communications from unauthorized sources.
4. **Disconnect from the Internet when you are away from your computer:** Attackers cannot get into the system when the system is disconnected from the Internet. Firewall, antivirus, and anti-Spyware softwares are not foolproof mechanisms to get access to the system.
5. **Downloading the freeware only from websites that are known and trustworthy:** It is always appealing to download free software(s) such as games, file-sharing programs, customized toolbars, etc. However, one should remember that many free software(s) contain other software, which may include Spyware.
6. **Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send:** If you do find such messages in your outbox, it is a sign that your system may have infected with Spyware, and maybe a part of a Botnet. This is not foolproof; many spammers have learned to hide their unauthorized access.
7. **Take an immediate action if your system is infected:** If your system is found to be infected by a virus, disconnect it from the Internet immediately. Then scan the entire system with fully updated antivirus and anti-Spyware software. Report the unauthorized accesses to ISP and to the legal authorities. There is a possibility that your passwords may have been compromised in such cases, so change all the passwords immediately.

2.7 Attack Vector

An “attack vector” is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome. Attack vectors enable attackers to exploit system vulnerabilities, including the human element. Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses. [14]

To some extent, firewalls and antivirus software can block attack vectors. However, no protection method is totally attack-proof. A defense method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers. Refer to Box 2.10.

Box 2.10 Zero-Day Attack

A zero-day (or zero-hour) attack^[17] is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e., undisclosed to the software vendor and software users) and/or for which no patch (i.e., security fix) is available. Zero-day exploits are used or shared by attackers before the software vendor knows about the vulnerability.

Sometimes software vendors discover the vulnerability but developing a patch can take time. Alternatively, software vendors can also hold releasing the patch reason to avoid the flooding the customers with numerous individual updates. A "zero-day" attack is launched just on or before the first or "zeroth" day of vendor awareness, reason being the vendor should not get any opportunity to communicate/distribute a security fix to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fixes commonly known as patches) are collected and then release them together as a package.

Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors.

Zero-day emergency response team (ZERT): This is a group of software engineers who work to release non-vendor patches for zero-day exploits. Nevada is attempting to provide support with the Zeroday Project at www.zerodayproject.com, which purports to provide information on upcoming attacks and provide support to vulnerable systems. Also visit the weblink <http://www.isotf.org/zert> to get more information about it.

Source: http://en.wikipedia.org/wiki/Zero_day_attack (9 October 2009).

The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware (refer to Chapter 4). If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

In the technical terms, *payload* is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs. From the technical perspective, payload does not include the “overhead” data required to get the packet to its destination. Payload may depend on the following point of view: “What constitutes it?” To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles. However, in more general usage, the payload is the bits that get delivered to the end-user at the destination.^[15,16]

The attack vectors described here are how most of them are launched.^[16,18]

1. **Attack by E-Mail:** The hostile content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something “free” or tempting is a suspect.
2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
3. **Attack by deception:** Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, hoaxes, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer’s operator to succeed. Social engineering and hoaxes are other forms of deception that are often an attack vector too.
4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use a variety of hacking tools, heuristics,

- and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.
5. **Headless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.
 6. **Attack of the worms:** Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses. Next they begin scanning the Internet from the computer they have just infected, and start looking for other computers to infect. If the worm is successful, it propagates rapidly. The worm owner soon has thousands of “zombie” computers to use for more mischief.
 7. **Malicious macros:** Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chat (IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.
 8. **Foistware (sneakware):** Foistware is the software that adds hidden components to the system on the sly. Spyware is the most common form of foistware. Foistware is quasi-legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some “revenue opportunity” that the foistware has set up.
 9. **Viruses:** These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

2.8 Cloud Computing

The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals. Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which makes it easier for cybercriminals to attack these systems.

Cloud computing is Internet (“cloud”)-based development and use of computer technology (“computing”).^[19] The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks. Cloud computing is a term used for hosted services delivered over the Internet. A cloud service has three distinct characteristics which differentiate it from traditional hosting:

1. It is sold on demand – typically by the minute or the hour;
2. it is elastic in terms of usage – a user can have as much or as little of a service as he/she wants at any given time;
3. the service is fully managed by the provider – a user just needs PC and Internet connection.

Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.

2.8.1 Why Cloud Computing?

The cloud computing has following advantages^[20]:

1. Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one user's computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space. Cloud computing gives the option of storing data on someone else's hardware, thereby removing the need for physical space on the front end.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware.

The cloud computing services can be either private or public. A public cloud sells services to anyone on the Internet (see Table 2.4 for cloud computing service providers). A private cloud is like a proprietary network or a data center that supplies the hosted services to a limited number of people. When a service provider uses public cloud resources to create a private cloud, the result is called a "virtual private cloud." The goal of cloud computing is to provide easy, scalable access to the computing resources and IT services.

Table 2.4 | Cloud computing service providers

<i>Sr. No.</i>	<i>Service Providers</i>	<i>Weblink</i>
1.	Amazon: It offers flexible, simple, and easy computing environment in the cloud that allows development of applications.	http://aws.amazon.com/ec2/
2.	3Tera: It offers AppLogic grid OS that enables infrastructure solutions according to the changing needs of business.	http://www.3tera.com/
3.	Force.com: It allows building of core business applications like enterprise resource planning (ERP), human resource management (HRM), and supply chain management (SCM).	http://www.salesforce.com/platform/
4.	Appistry-Cloud Computing Middleware: It allows easily scalable cloud computing for a wide variety of applications and services for both public and private clouds.	http://www.appistry.com/
5.	Microsoft Live Mesh: This cloud setup synchronizes the files with the all users' devices like laptop, Mac, mobile phone, or others and allows to access the files from any device as well as enables sharing of files.	<a "="" href="https://www.mesh.com>Welcome/default.aspx</td></tr><tr><td>6.</td><td>AppNexus: This helps a user to launch several operating systems, run a variety of applications, load balance these applications, and store huge amount of secure data.</td><td>http://www.appnexus.com/

(Continued)

Table 2.4 | (Continued)

<i>Sr. No.</i>	<i>Service Providers</i>	<i>Weblink</i>
7.	Flexiscale: It is self-service through control panel or API – features full self-service – start/stop/delete, change memory/CPU/storage/IPs of virtual dedicated servers.	http://www.flexiscale.com/
8.	GoogleApp Engine: This is a free setup that allows the users to run their web application on Google infrastructure.	http://www.google.com/apps/intl/en/business/index.html
9.	GoGrid: It offers unique multiserver control panel that enables the user to deploy and manage load-balanced cloud servers.	http://www.gogrid.com/
10.	Terremark Enterprise Cloud: It provides the power to the user for computing resources for user's mission-critical applications.	http://www.terremark.com/services/cloudcomputing/theenterprisecloud.aspx

Source: <http://blog.taragana.com/index.php/archive/top-10-cloud-computing-service-provider/> (9 October 2009).



Although cloud computing is an emerging field, the idea has been evolved over few years. It is called cloud computing because the data and applications exist on a “cloud” of Web servers.

2.8.2 Types of Services

Services provided by cloud computing are as follows^[19]:

1. **Infrastructure-as-a-service (IaaS):** It is like Amazon Web Services that provide virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an Application Programmable Interface (API) from which they can control their servers. As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.
2. **Platform-as-a-service (PaaS):** It is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs. Google Apps is one of the most famous PaaS providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.
3. **Software-as-a-service (SaaS):** It is the broadest market. In this case, the provider allows the customer only to use its applications. The software interacts with the user through a user interface. These applications can be anything from Web-based E-Mail to applications such as Twitter or Last.fm.

2.8.3 Cybercrime and Cloud Computing

Nowadays, prime area of the risk in cloud computing is protection of user data. See Table 2.5 to understand major areas of concerns in cloud computing domain.

Table 2.5 | Risks associated with cloud computing environment

<i>Sr. No.</i>	<i>Area</i>	<i>What is the Risk?</i>	<i>How to Remediate the Risk?</i>
1.	Elevated user access	Any data processed outside the organization brings with it an inherent level of risk, as outsourced services may bypass the physical, logical, and personnel controls and will have elevated user access to such data.	Customer should obtain as much information as he/she can about the service provider who will be managing the data and scrutinizing vendor's monitoring mechanism about hiring and oversight of privileged administrators, and IT controls over the access privileges.
2.	Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments. This can result into non-compliance with various standards/laws like the US government's Health Insurance Portability and Accountability Act (HIPAA), or Sarbanes-Oxley; the European Union's Data Protection Directive or the credit card industry's Payment Card Industry Data Security Standard (PCI DSS).	The organization is entirely responsible for the security and integrity of their own data, even when it is held by a service provider. Hence, organization should force cloud computing service providers to undergo external audits and/or security certifications and submit the report on periodic basis.
3.	Location of the data	The organizations that are obtaining cloud computing services may not be aware about where the data is hosted and may not even know in which country it is hosted.	Organizations should ensure that the service provider is committed to obey local privacy requirements on behalf of the organization to store and process the data in the specific jurisdictions.
4.	Segregation of data	As the data will be stored under stored environment, encryption mechanism should be strong enough to segregate the data from other organizations, whose data are also stored under the same server.	Organization should be aware of the arrangements made by the service provider about segregation of the data. In case of encryption mechanism, the service provider should display encryption schemes and testing of the mechanism by the experts.
5.	Recovery of the data	Business continuity in case of any disaster – availability of the services and data without any disruption. Application environment and IT infrastructure across multiple sites are vulnerable to a total failure.	Organization should ensure the enforcement of contractual liability over the service provider about complete restoration of data within stipulated timeframe. Organization should also be aware of Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) established by the service provider.
6.	Information security violation reports	Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity.	Organization should enforce the contractual liability toward providing security violation logs at frequent intervals.
7.	Long-term viability	In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.	Organization should ensure getting their data in case of such major events.

The risk areas identified in Table 2.5 are considered to be key obstacles to adoption of cloud computing and making it an area of active research across the globe.

SUMMARY

In this chapter we have discussed how technology is used in a different way for conducting illegal activities against a person, property, and/or organizations including governments. Considerable amount of time is spent in gathering information about a target. Therefore, one should have adequate knowledge about the technology to use, the different tools and techniques. Public networks and cybercafes are used to hide the ID for information gathering as well as launching attacks and hence it becomes important to take utmost care while operating/surfing through such facilities. People are the weakest link in the security domain and, hence, they get either exploited/deceived

to obtain the required information; thus, this is called social engineering. Cyberstalking is another way through which criminals interact with victims directly, avoiding face-to-face conversation. Criminals do this either for harassing and/or threatening behavior or to get the information from the victim. The Internet has become an integral part of the lifestyle nowadays and IT is found to be pervasive – the result is cloud computing; however, we should also be aware of threats inducing from such technologies like Botnets and attack vectors. Every technology has some limitations and attackers having good amount of knowledge will always try to exploit it.

REVIEW QUESTIONS

- How are cybercrimes classified? Explain with examples.
- Explain the difference between passive and active attacks. Provide examples.
- What is social engineering?
- What is cyberstalking? As per your understanding is it a crime under the Indian IT Act?
- Explain how Botnets can be used as a fuel to cybercrime.
- What are the different attacks launched with attack vector. Explain.
- Explain cloud computing and cybercrime.

REFERENCES

- To know more on patriot hacking, visit: http://en.wikipedia.org/wiki/Patriot_hacking (25 June 2009).
- To know more on port scanner, visit: http://en.wikipedia.org/wiki/Port_scanner (10 February 2010).
- To know more on cyberstalking, visit: <http://en.wikipedia.org/wiki/Cyberstalking> (2 April 2009).
- To know more on cyberbullying, visit: <http://en.wikipedia.org/wiki/Cyber-bullying> (2 April 2009).
- To know more on cyberstalking, visit: <http://cyberlaws.net/cyberindia/2CYBER27.htm> (2 April 2009).
- To know more on cybercafe, visit: <http://www.business-standard.com/india/news/cyber-cafe-audience-captive-power/351936/> (25 June 2009).
- To know more on cybercafe, visit: <http://www.merinews.com/catFull.jsp?articleID=155371> (25 June 2009).
- To know more on cybercafe, visit: <http://punekar.in/site/2009/02/04/city-cyber-cafes-install-deep-freeze-software-for-security/> (27 June 2009).

- [9] To know more on cybercafe, visit: <http://www.icicibank.com/pfsuser/temp/cybersec.htm> (27 June 2009).
- [10] To know more on cybercafe, visit: <http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm> (27 June 2009).
- [11] To know more on Botnet, visit: <http://en.wikipedia.org/wiki/Botnet> (19 March 2009).
- [12] To know more on Botnet, visit: <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt132.shtm> (30 March 2009).
- [13] To know more on Botnet, visit: <http://www.viruslist.com/en/analysis?pubid=204792068> (30 March 2009).
- [14] To know more on attack vector, visit: <http://searchsecurity.techtarget.com/dictionary/definition/1005812/attack-vector.html#> (17 July 2009).
- [15] To know more on attack vector, visit: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214475,00.html (17 July 2009).
- [16] To know more on attack vector, visit: <http://www.net-security.org/article.php?id=949> (17 July 2009).
- [17] To know more on zero-day attack, visit: http://en.wikipedia.org/wiki/Zero_day_attack (9 October 2009).
- [18] To know more on attack vector, visit: <http://cybercoyote.org/security/vectors.shtml> (17 July 2009).
- [19] To know more on cloud computing, visit: http://en.wikipedia.org/wiki/Cloud_computing (9 October 2009).
- [20] To know more on cloud computing, visit: <http://communication.howstuffworks.com/cloud-computing2.htm> (9 October 2009).

FURTHER READING

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Graves, K. (2007) *CEH – Official Certified Ethical Hacker Review Guide*, Wiley Publishing Inc., IN, USA.
3. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, C, D, E, F, J, L. These are provided in the companion CD.

3

Cybercrime: Mobile and Wireless Devices

Learning Objectives

After reading this chapter, you will be able to:

- Understand the security challenges presented by mobile devices and information systems access in the cybercrime world.
 - Understand the challenges faced by the mobile workforce and their implications under the cybercrime era.
 - Get an overview on mitigation strategy like the CLEW for possible protection of credit card users.
 - Learn about security issues arising due to use of media players.
 - Understand the organizational security implications with electronic gadgets and learn what organizational measures need to be implemented for protecting information systems from threats in mobile computing area.
 - Understand Smishing and Vishing attacks in the Mobile World.
 - Understand the security issues arising due to daily use of removable media such as pen/zip drives in this mobile environment.
-

3.1 Introduction

In this modern era, the rising importance of *electronic gadgets* (i.e., mobile hand-held devices) – which became an integral part of business, providing connectivity with the Internet outside the office – brings many challenges to secure these devices from being a victim of cybercrime. In the recent years, the use of laptops, personal digital assistants (PDAs), and mobile phones has grown from limited user communities to widespread desktop replacement and broad deployment. According to Quocirca Insight Report (2009),^[1] by the end of 2008 around 1.5 billion individuals around the world had the Internet access. In November 2007, mobile phone users were numbered 3.3 billion, with a growing proportion of those mobile devices enabled for the Internet access. The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address. Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart hand-held devices such as PDAs have become networked, converging with mobile phones. Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the *Smartphone*.

Smartphones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool. Although IT departments of organizations as yet are not swapping employees' company-provided

PDAs (as the case may be) for the Smartphones, many users may bring these devices from home and use them in the office. Research in Motion's (RIM) BlackBerry Wireless Hand-held is an alternate technology. According to Research in Motion Annual Report (2009),^[2] there are over 175,000 organizations with BlackBerry Enterprise Server installed behind the corporate firewall (i.e., corporations that use the BlackBerry enterprise server and client/server software for data communication between corporate BlackBerry devices and other mail systems). Thus, the larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity. Clearly, these technological developments present a new set of security challenges to the global organizations.

3.2 Proliferation of Mobile and Wireless Devices

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices. Figure 3.1 shows some typical hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure 3.2 helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.



Figure 3.1 Typical hand-held devices.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

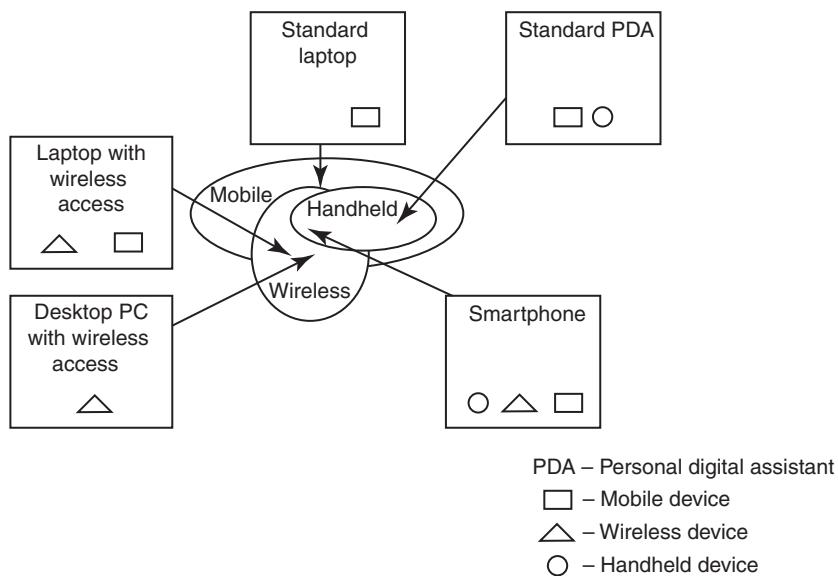


Figure 3.2 Mobile, wireless and hand-held devices.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Mobile computing is “taking a computer and all necessary files and software out into the field.” Many types of mobile computers have been introduced since 1990s.^[3] They are as follows:

- Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some “setting-up” and an AC power source.
- Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch-screen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
- Internet tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
- Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
- Ultramobile PC:** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
- Smartphone:** It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
- Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound system, *global positioning system* (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
- Fly Fusion Pentop computer:** It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection. Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted to a desktop, that is, not tethered. As more personal devices find their way into the enterprise, corporations are realizing cybersecurity threats that come along with the benefits achieved with mobile solutions.

Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all. Thus, while “wireless” is a subset of “mobile,” in most cases, an application can be mobile without being wireless. Smart hand-helds are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network, and can have software installed on them; this includes networked PDAs and Smartphones. In this chapter the term “hand-held” is used as an all-embracing term.

3.3 Trends in Mobility

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. “iPhone” from Apple and Google-led “Android” phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain. Figure 3.3 shows the different types of mobility and their implications.

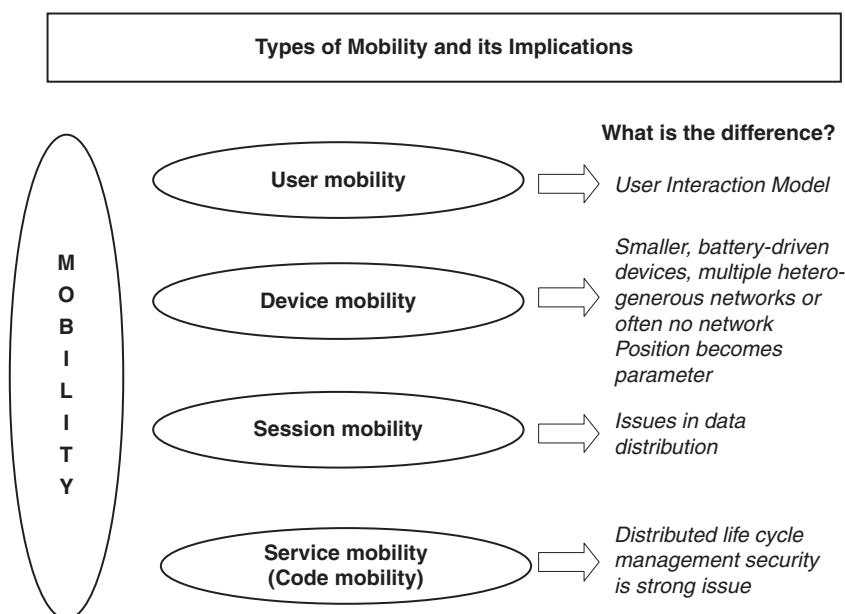


Figure 3.3 | Mobility types and implications.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

To assess major challenges in the mobility domain, let us see the statistics found during the surveys. In one such survey,^[4] reported by Quocirca, employees working in government departments have lost or mislaid over 1,000 laptops, lost more than 500 phones or mobile E-Mail gadgets and lost over 700 other mobile devices (i.e., probably memory sticks, cameras, etc.). Another such survey, reported by Quocirca,^[5] of the 2,853 respondents, 29% had a broad experience of wireless laptops, 14% had a broad experience of smart hand-holds, with around a further 60% in each case having a more limited or unofficial experience. Findings from surveys like these help us demystify many perceptions about mobile and wireless connectivities. The results of surveys like these indicate that we are grappling with a “perception problem”; most people have not as yet come to terms with the fact that the hand-held devices may look “harmless” but they can cause serious cybersecurity issues to the organizations (see Box 3.1).

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network – that is, public Internet, private networks and other operator’s networks – and the other is within the mobile networks – that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Box 3.1 Key Findings for Mobile Computing Security Scenario

1. **With usage experience, awareness of mobile users gets enhanced:** Survey showed that those with broad wireless laptop experience place less emphasis on this aspect for the deployment of smart hand-holds. However, an experience of small hand-held deployment boosted the numbers seeing the need for increased provision of user support and training.
2. **People continue to remain the weakest link for laptop security:** Antivirus software, secured virtual private network (VPN) access and personal firewalls are deployed over two-thirds of IT professionals, but those with a broad wireless experience regard loss, damage or unauthorized use as their major concerns. These depend on the care taken by the users and well-communicated security policies.
3. **Wireless connectivity does little to increase burden of managing laptops:** The cost and complexity of device management is seen as an issue by around half of the IT professionals surveyed. However, the level of challenge perceived to affect security, device management and use support is unaffected by a broader experience of wireless laptop deployment.
4. **Laptop experience changes the view of starting a smart hand-held pilot:** The key concerns for starting a smart hand-held are security and the cost of devices, but these lessen for those with a broad wireless laptop experience. However, the concern over choosing the most appropriate devices rises with experience; users cite further concerns over interoperability and compatibility.
5. **There is naivety and/or neglect in smart hand-held security:** Although plenty of emphasis is placed on security, a large number of IT departments do not enforce security for smart hand-holds as well as for laptops or they leave it in the hands of the users. This is more prevalent in those with limited or unofficial smart hand-held activity, but even those with a broad experience (almost one-third of those surveyed) do not treat smart hand-held security as seriously as laptops.
6. **Rules rather than technology keep smart hand-holds' usage in check:** Businesses with an existing experience of smart hand-holds favored a policy of controlled deployment, with almost two-thirds of those surveyed providing a limited choice of devices, and only one-third of the surveyed population was user of technology solution based on continuous synchronization. However, broad experience increases the use of other automated solutions, such as centralized software management and remote device deactivation.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Popular types of attacks against 3G mobile networks^[6] are as follows:

1. **Malwares, viruses and worms:** Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:
 - *Skull Trojan:* It targets Series 60 phones equipped with the Symbian mobile OS.
 - *Cabir Worm:* It is the first dedicated mobile-phone worm; infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
 - *Mosquito Trojan:* It affects the Series 60 Smartphones and is a cracked version of “Mosquitos” mobile phone game.
 - *Brador Trojan:* It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conducive to traditional worm propagation vector such as E-Mail file attachments (refer to Appendix C).
 - *Lasco Worm:* It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir’s source code and replicates over Bluetooth connection.
2. **Denial-of-service (DoS):** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable (we will address this attack in detail under Chapter 4). Presently, one of the most common cyber-security threats to wired *Internet service providers* (ISPs) is a distributed denial-of-service (DDoS) attack. DDoS attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped. Botnets/zombies are used to create enough traffic to impose that kind of damage (we have addressed zombies in Chapter 1 and Botnets in Chapter 2).
3. **Overbilling attack:** Overbilling involves an attacker hijacking a subscriber’s IP address and then using it (i.e., the connection) to initiate downloads that are not “Free downloads” or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.
4. **Spoofed policy development process (PDP):** These types of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].
5. **Signaling-level attacks:** The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

To know more on this topic, readers may visit http://www.igr-inc.com/uploads/free_white_papers/3G_MobileSecurity_Jan07.pdf



Mobile Security Processing System (MOSES) is a programmable security processor platform that enables secure data and multimedia communications in next-generation wireless mobile computing. MOSES was developed to meet the security challenges in emerging mobile technology such as 3G and 4G mobile phones and PDAs. It is a security processing architecture to provide secure (i.e., tamper-resistant) and efficient (i.e., high performance, low power) execution of security processing functions. It constitutes three key components, such as Security Processing Engine (SPE), a hierarchical secure memory subsystem and security-enhanced communication architecture, from hardware perspective.

3.4 Credit Card Frauds in Mobile and Wireless Computing Era

These are new trends in cybercrime that are coming up with mobile computing – mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. *Mobile credit card transactions* are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.

Today belongs to “mobile computing,” that is, *anywhere anytime computing*. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment. These businesses include mobile utility repair service businesses, locksmiths, mobile windshield repair and others. Some upscale restaurants are using wireless processing equipment for the security of their credit card paying customers. Figure 3.4 shows the basic flow of transactions involved in purchases done using credit cards.^[7] Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems (refer to Chapter 5) once they occur. But they could reduce ID fraud even more if they give consumers better tools to monitor their accounts and limit high-risk transactions (Box 3.2).

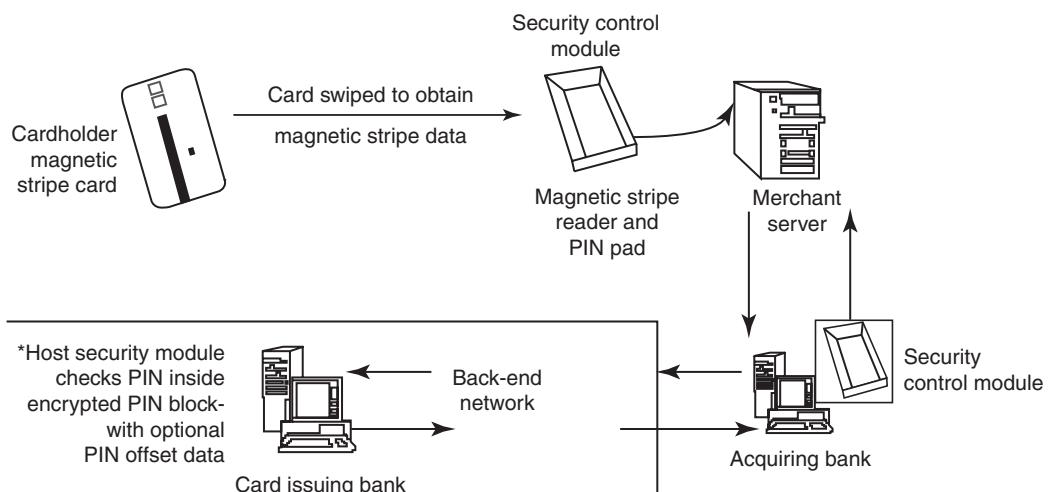


Figure 3.4 | Online environment for credit card transactions.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.2 Tips to Prevent Credit Card Frauds

The current topic is about credit card frauds in mobile and wireless computing era, however, we would like to include these tips to prevent credit card frauds^[8] caused due to individual ignorance about a few known facts.

Do's

1. Put your signature on the card immediately upon its receipt.
2. Make the photocopy of both the sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.
3. Change the default personal identification number (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.
7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.

Dont's

1. Store your card number and PINs in your cell.
2. Lend your cards to anyone.
3. Leave cards or transaction receipts lying around.
4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).
5. Write your card number/PIN on a postcard or the outside of an envelope.
6. Give out immediately your account number over the phone (unless you are calling to a company/to your bank).
7. Destroy credit card receipts by simply dropping into garbage box/dustbin.

Source: <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre07.shtm>

There is a system available from an Australian company “Alacrity” called closed-loop environment for wireless (CLEW). Figure 3.5 shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.^[9]

As shown in Figure 3.5, the basic flow is as follows:

1. Merchant sends a transaction to bank;
2. the bank transmits the request to the authorized cardholder [*not* short message service (SMS)];
3. the cardholder approves or rejects (password protected);
4. the bank/merchant is notified;
5. the credit card transaction is completed.

3.4.1 Types and Techniques of Credit Card Frauds

Traditional Techniques

The traditional^[10] and the first type of credit card fraud is paper-based fraud – *application fraud*, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information (PII) (refer to Chapter 5) to open an account in someone else's name.

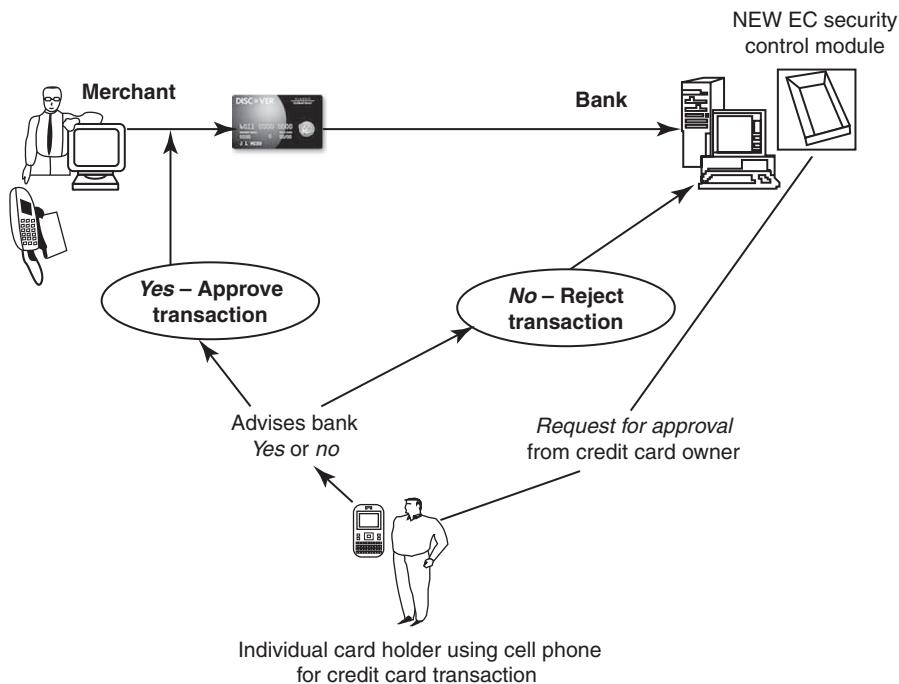


Figure 3.5 | Closed-loop environment for wireless (CLEW).

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.3 Potential Wireless Users – Beware!

Although wireless processing is a very good system for many companies, however, it is not for all mobile businesses. There are some drawbacks to wireless processing that many potential wireless users should be aware of before they venture into wireless processing. They are as follows:

- Wireless processing equipment is expensive:** There is no way to get around this. Wireless credit card machines are the most advanced processing terminals available. You get what you pay for! For a wireless terminal with a printer, expect to pay at least US\$ 800 for a new terminal and US\$ 700 for a refurbished terminal. If you are purchasing a terminal that is much cheaper than any other you find, it is most likely outdated equipment that uses outdated cellular networks. In other words, it is a scam, and you are about to buy a really expensive paperweight.
- Wireless processing comes with extra fees:** Just like a cell phone, wireless credit card machines operate on cellular networks. You have to pay for this cellular service in addition to the high cost of equipment. Luckily, wireless fees for processing are nowhere near what they are for cell phones. Expect to pay US\$ 20–25 per month for a wireless service fee.
- Wireless credit card machines are subject to cellular coverage blackouts:** I know what you are thinking – “My cell phone works almost everywhere, so my wireless credit card machine will too.” Sadly, this is not the case. Wireless credit card processing uses a business cellular network called the Motient or Mobitex network. Your cell phone may be using a network called code division multiple access (CDMA) or time division multiple access (TDMA) [global system for mobile communications (GSM)] or some other technology-based network. The coverage that your cell phone gets is much greater than the wireless processing network. There can be some states in your country with no coverage for wireless processing at all.

Box 3.3 Potential Wireless . . . (Continued)

4. **You cannot process checks or debit transactions over a wireless network:** Currently owing to federal regulations, it is impossible to process debit transaction or electronic checks over a wireless network. This is something that will probably end up being allowed in the future, but as of now there is not sufficient security or encryption to process these transactions wireless.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Application fraud can be divided into

1. **ID theft:** Where an individual pretends to be someone else (see more on ID Theft in Chapter 5).
2. **Financial fraud:** Where an individual gives false information about his or her financial status to acquire credit.

Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

Modern Techniques

Sophisticated techniques^[10] enable criminals to produce fake and doctored cards. Then there are also those who use skimming to commit fraud. Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another (see more on skimming frauds in Chapter 11 in CD). Site cloning and false merchant sites on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing (see more on this in Chapter 5). Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink/website (i.e., they have been scammed).

1. **Triangulation:** It is another method of credit card fraud and works in the fashion as explained further.
 - The criminal offers the goods with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.
 - The customer registers on this website with his/her name, address, shipping address and valid credit card details.
 - The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address that have been provided by the customer while registering on the criminal's website.
 - The goods are shipped to the customer and the transaction gets completed.
 - The criminal keeps on purchasing other goods using fraudulent credit card details of different customers till the criminal closes existing website and starts a new one.

Such websites are usually available for few weeks/months, till the authorities track the websites through which the criminal has enticed the individuals to reveal their personal details, which enabled the criminal to commit the transactions by using the credit card details of these customers. The entire investigation process for tracking and reaching these criminals is time-consuming, and the criminals may close such fake website in between the process that may cause further difficulty to trace the criminal. The criminals aim to create a great deal of confusion for the authorities so that they can operate long enough to accumulate a vast amount of goods purchased through such fraudulent transactions.

2. **Credit card generators:** It is another modern technique – computer emulation software – that creates valid credit card numbers and expiry dates. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

3.5 Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important issues in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in Fig. 3.6.

As the number of mobile device users increases, two challenges are presented: one at the device level called “microchallenges” and another at the organizational level called “macrochallenges.” Of these, some microchallenges are discussed in this section and macrochallenges in the next section.

Some well-known technical challenges in mobile security are: *managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API) security, etc.* In this section, we provide a brief discussion on these cybersecurity aspects. For most of the discussion here, the reference point is Windows mobile development given that the developers of the Windows OS are on the forefront of the technology in terms of their mobile computing technological initiatives. In view of the discussion in Section 3.4, the ID theft (we will address it in Chapter 5) is now becoming a major fraud in credit card business domain, wherein individual’s *Personally Identifiable Information (PII)* is misused to open new credit accounts, take new loans or engage in other types of frauds, such as misuse of the victim’s

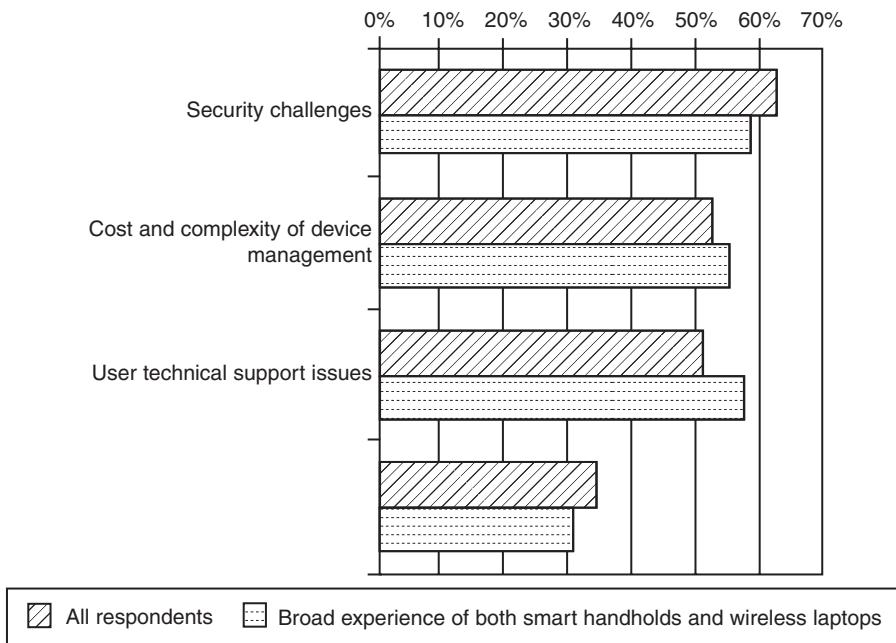


Figure 3.6 | Important issues for managing mobile devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

name and identifying information when someone is charged with a crime, when renting an apartment or when obtaining medical care.

3.6 Registry Settings for Mobile Devices

Let us understand the issue of registry settings on mobile devices through an example: Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device. In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context,

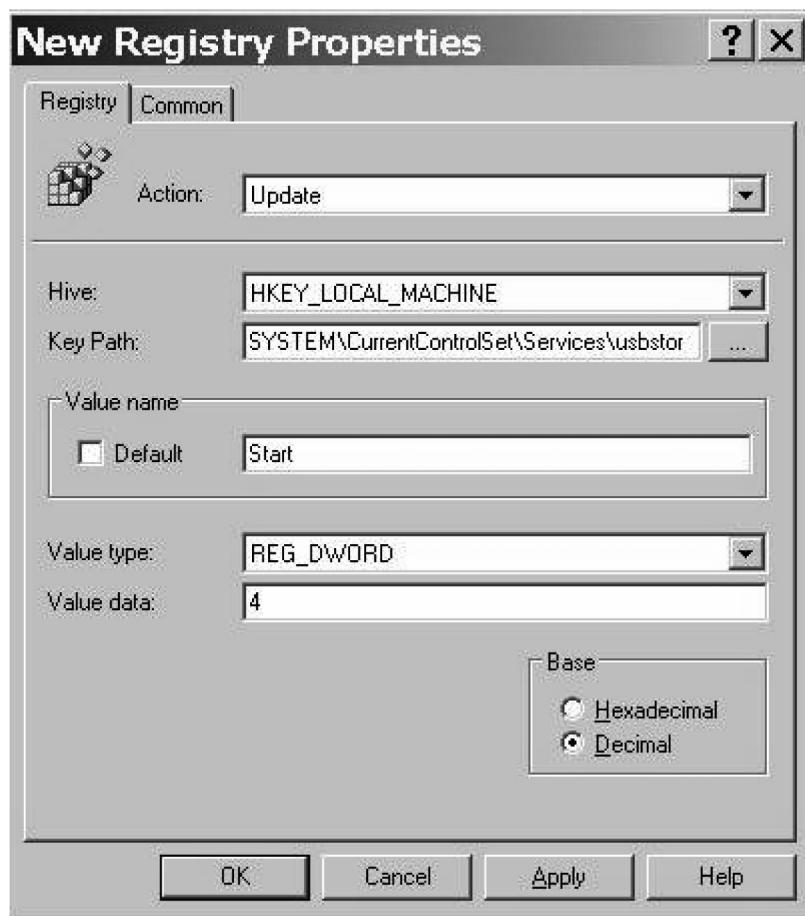


Figure 3.7 | Registry value browsing.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within “group policy.” Group policy is one of the core operations that are performed by Windows Active Directory. As a supporting point, consider the following: within the last 2 years, Microsoft has doubled the number of group policy settings that it ships with the OS. There are now nearly 1,700 settings in a standard group policy. The emphasis on most of the group policy settings is security.

There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against *Spyware, viruses, worms, malware* (we will address it in Chapter 4) and other Malicious Codes that run through the networks and the Internet. Microsoft and other companies are trying to develop solutions as fast as they can, but the core problem is still not being addressed. According to the experts, the core problem to many of the mobile security issues on a Windows platform is that the baseline security is not configured properly. When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every *Control Panel setting* and *group policy* option, they may not get the computer to the desired baseline security. For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional *registry* changes that are not exposed through any interface. There are many ways to complete these registry changes on every computer, but some are certainly more efficient than others.

Naive users may think that for solving the problem of mobile device security there are not many registry settings to tackle. However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of “registry hacks” that are discussed in Microsoft Knowledge Base articles. Figure 3.7 displays an illustration of how some tools allow users to browse to the desired registry value on their mobile devices.

3.7 Authentication Service Security

There are two components of security in mobile computing: *security of devices* and *security in networks*. A secure network access involves mutual authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices. Some eminent kinds of attacks to which mobile devices are subjected to are: *push attacks, pull attacks* and *crash attacks* (see Figs. 3.8–3.10).

Authentication services security is important given the typical attacks on mobile devices through wireless networks: *DoS attacks, traffic analysis, eavesdropping, man-in-the-middle attacks* and *session hijacking*. We will continue further technical discussion on such topics in Chapter 4. Security measures in this scenario come from *Wireless Application Protocols* (WAPs), use of *VPNs*, *media access control (MAC) address filtering* and development in 802.xx standards.

3.7.1 Cryptographic Security for Mobile Devices

In this section we will discuss a technique known as *cryptographically generated addresses* (CGA). CGA is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner’s public-key address. The address the owner uses is the corresponding private key to assert address ownership

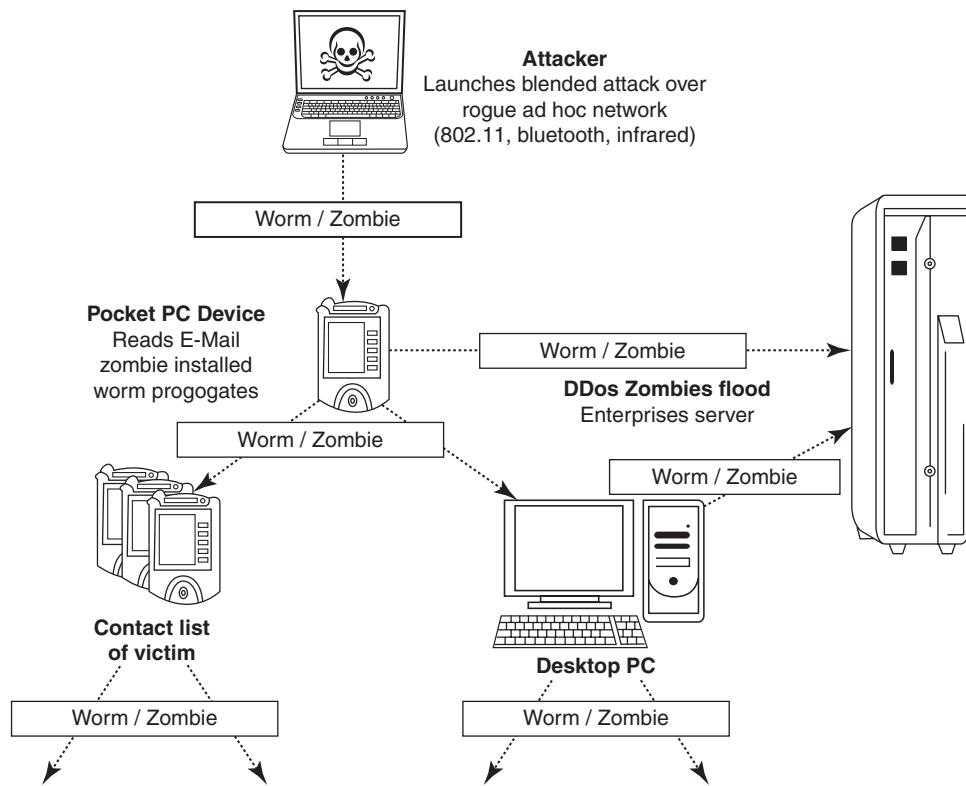


Figure 3.8 Push attack on mobile devices. DDoS implies distributed denial-of-service attack.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure. Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices. CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in *context-aware mobile computing applications*) and mobility protocols. It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms (devices that can be held in one's palm, illustrated in Fig. 3.1) are one of the most common hand-held devices used in mobile computing. *Cryptographic security controls* are deployed on these devices. For example, the *Cryptographic Provider Manager* (CPM) in Palm OS5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

3.7.2 LDAP Security for Hand-Held Mobile Computing Devices

LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network (i.e., on the public Internet or on the organization's Intranet). In a network, a directory tells you where an entity is located in the network. LDAP is a light weight (smaller

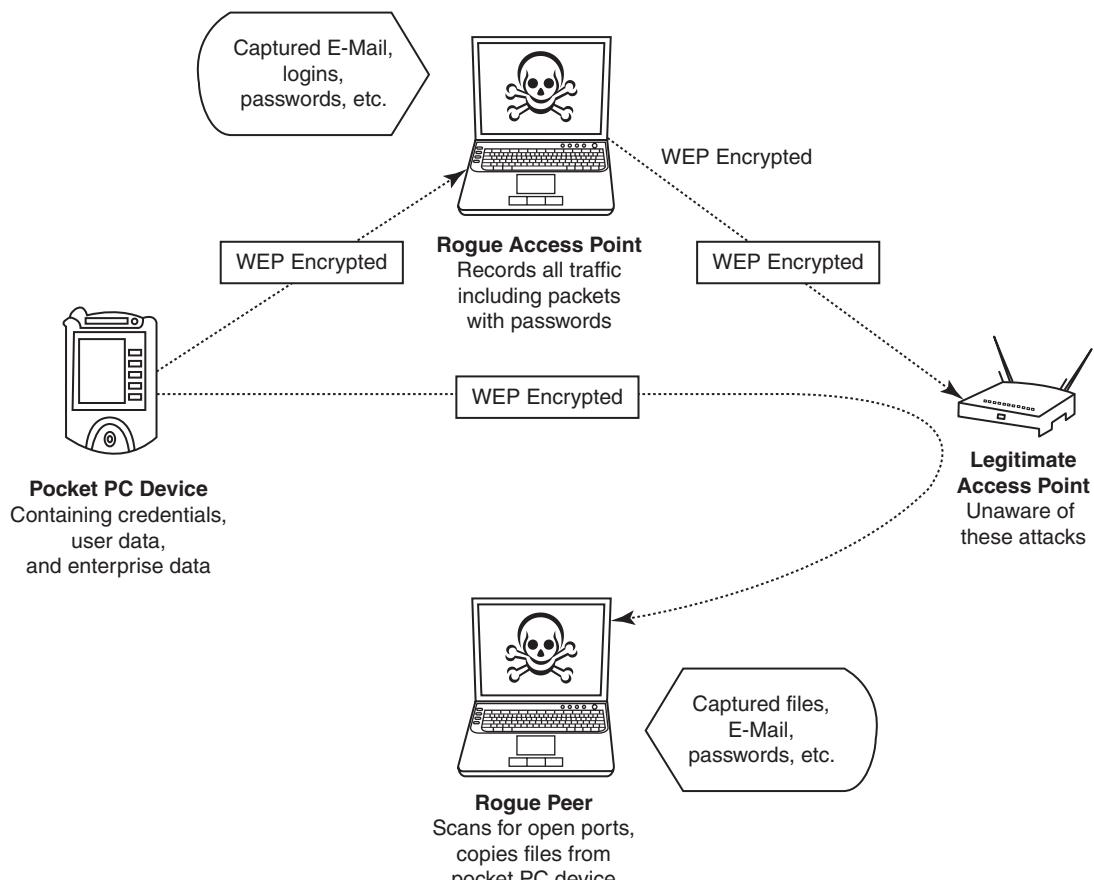


Figure 3.9 | Pull attack on mobile devices.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

amount of code) version of Directory Access Protocol (DAP) because it does not include security features in its initial version. It originated at the University of Michigan and has been endorsed by at least 40 companies. Centralized directories such as LDAP make revoking permissions quick and easy. Box 3.4 describes the directory structure of LDAP.

3.7.3 RAS Security for Mobile Devices

RAS is an important consideration for protecting the business-sensitive data (refer to Chapter 5) that may reside on the employees' mobile devices. In terms of cybersecurity, mobile devices are sensitive. Figure 3.11 illustrates how access to an organization's sensitive data can happen through mobile hand-held devices carried by employees. In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user (*impersonating or masquerading*) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.

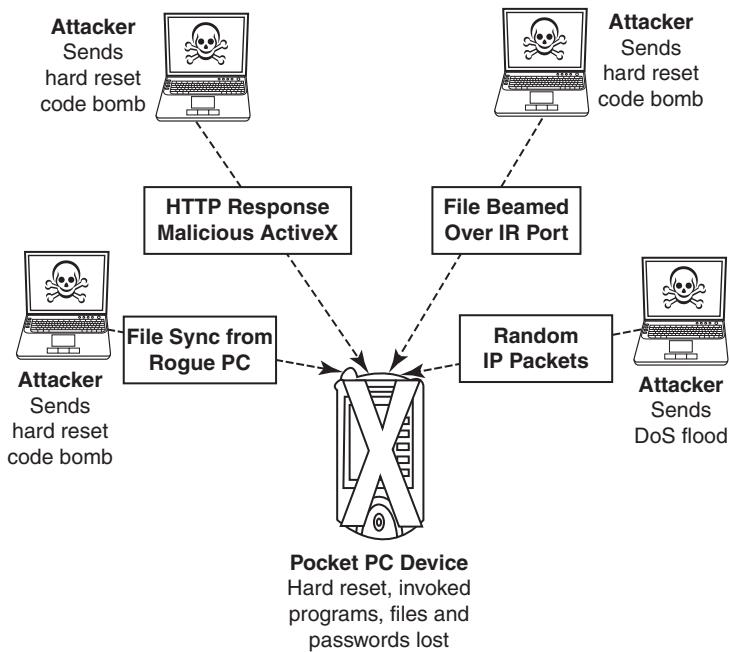


Figure 3.10 Crash attack on mobile devices. DoS – Denial-of-service attack.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.4 LDAP Directory Structure

An LDAP directory is organized into a simple "tree" structure that consists of the following levels:

1. Root Directory (the source of the tree or the starting point) which branches out to
2. Countries, which branches out to
3. Organizations, which branches out to
4. Organizational units (divisions/departments and so forth), which further branches out to
5. Individuals (which, in turn, include files, shared IT resources such as printers and people)

An LDAP server is called a *Directory Systems Agent* (DSA). It receives a request from a user, takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user. An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically.

Source: <http://www.csgnetwork.com/glossaryl.html>

Another threat comes from the practice of *port scanning* (refer to Box 2.5 in Chapter 2). First, attackers use a domain name system (DNS) server to locate the *IP address* of a connected computer (either the mobile device itself or a gateway server to which it connects). A *domain* is a collection of sites that are related in some sense. Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls. For instance, *File Transfer Protocol* (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by the attackers (see Box 3.5).

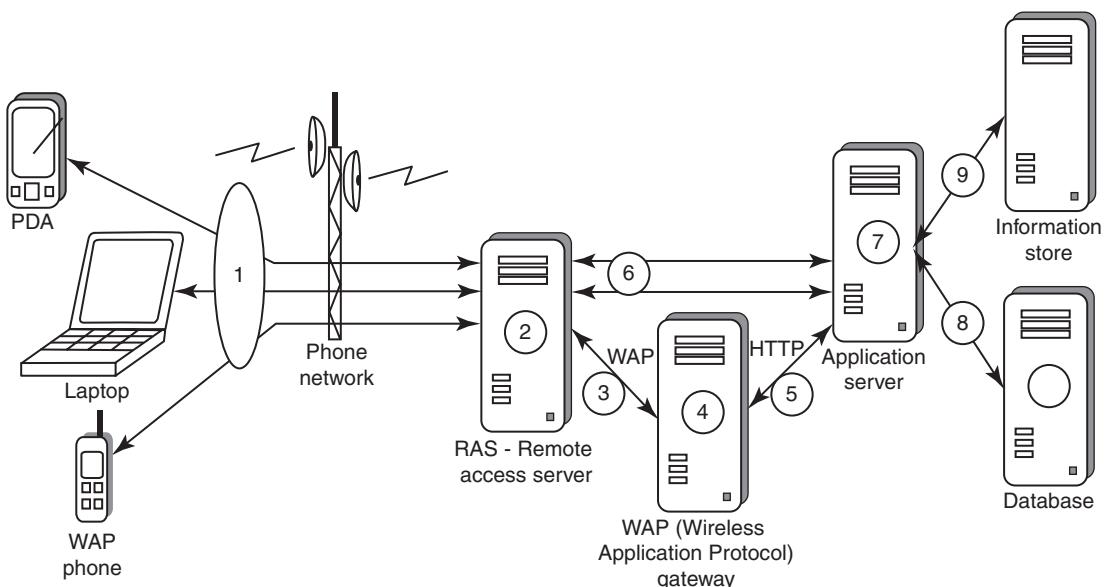


Figure 3.11 Communication from mobile client to organization information store.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.5 RAS System Security for Mobile Device Clients

The security of a RAS system can be divided into following three areas:

1. The security of the RAS server;
2. the security of the RAS client;
3. the security of data transmission.

Although the desired level of security of the RAS server can be controlled through implementation of local security guidelines, the RAS client (e.g., a mobile hand-held device) is typically not under the complete control of the IT personnel who is responsible for the local area network (LAN). The security of the data transmission media is generally completely out of their control. For this reason, protection of communications between the client and the server must be secured by additional means.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID. A *personal firewall* on a pocket PC or Smartphone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection. For situations where all connections to the corporate network pass through a gateway, placing the personal firewall on the gateway itself could be the simplest solution, because it avoids the need to place a personal firewall on each mobile device. In either case, deploying secure access methods that implement *strong authentication keys* will provide an additional protection.

3.7.4 Media Player Control Security

Given the lifestyle of today's young generation, it is quite common to expect them embracing the mobile hand-held devices as a means for information access, remote working and entertainment. Music and video are the two important aspects in day-to-day aspects for the young generation. Given this, it is easy to appreciate how this can be a source for cybersecurity breaches. Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the "music gateways." There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices. For example, in the year 2002, Microsoft Corporation warned about this.^[11] According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack people's computer systems and perform a variety of actions. According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.

As another example, consider the following news item of the year 2004: corrupt files posing as normal music and video files could allow an attacker to gain control of the downloader's computer (see Ref. #5, Additional Useful Web References, Further Reading). With this happening, there are three vulnerabilities: (a) files could be created that will open a website on the user's browser (e.g., the user could be accessing from his/her hand-held device) from where remote JavaScript can be operated; (b) files could be created which allow the attacker to download and use the code on a user's machine or (c) media files could be created that will create buffer overrun errors. We will continue further technical discussion on "buffer overflow" in Chapter 4.

In Section 3.6, we have discussed registry settings in connection with the mobile devices' security. This topic becomes important in the context of the current section too. Registry of a computing device is an important concept; it stores information necessary to configure the system for applications and hardware devices. It also contains information that the OS continually references during an operation. In the registry, some keys control the behavior of the Windows Media Player control. Microsoft, through its developer network MSDN, describes details of registry value settings on the mobile devices. With the increase in our mobile workforce and the resulting increase in the number of mobile computing hand-held devices used by the young employees of most IT and software organizations, it would be quite common to expect such cybersecurity attacks and hence one should be ready for security measures.

3.7.5 Networking API Security for Mobile Computing Applications

With the advent of electronic commerce (E-Commerce) and its further off-shoot into *M-Commerce*, online payments are becoming a common phenomenon with the *payment gateways* accessed remotely and possibly wirelessly. Furthermore, with the advent of *Web services* and their use in mobile computing applications (see Ref. #3, Articles and Research Paper, Further Reading), the API becomes an important consideration.

Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.

Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices). Technological developments such as these provide the ability to significantly improve cybersecurity of a wide range of consumer as well as mobile devices. Providing a common software framework, APIs will become an important enabler of new and higher value services.

3.8 Attacks on Mobile/Cell Phones

3.8.1 Mobile Phone Theft

Mobile phones have become an integral part of everybody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims. When anyone loses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)" (refer to Chapter 5), that really matter, are lost. Refer to Box 3.6 to learn about tips on securing mobile phone from being stolen and/or lost.

One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement. After PC, the criminals' (i.e., attackers')

Box 3.6

Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

Nowadays, mobiles/cell phones are becoming fancier and expensive hence increasingly liable to theft. Criminals are interested in accessing wireless service and seek potential possibility to stealing the ID.

Ensure to note the following details about your cell phone and preserve it in a safe place^[12]:

1. Your phone number;
2. the make and model;
3. color and appearance details;
4. PIN and/or security lock code;
5. IMEI number.

The International Mobile Equipment Identity (IMEI)

It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number and can be obtained by entering *#06# from the keypad.

The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country. For example, if a mobile phone is stolen, the owner can call his or her service provider and instruct them to "lock" the phone using its IMEI number. This will help to stop the usage of phone in that country, even if a SIM is changed.

Visit the weblink <http://www.numberingplans.com/?page=analysis&sub=imeinr> to check all information about your cell phone such as manufacturer, model type and country of approval of a handset.

1. Add a security mark on your cell phone. Use permanent marker and print your alternate contact number and short address on your cell phone instrument as well as on battery. In case someone finds your handset, it is easier to contact you if the finder of your cell phone would like to return it to you.
2. Set a password and ensure the password is strong enough so that a finder of your cell phone cannot easily guess it.
3. In case of loss of your cell phone, register a complaint with cell phone service provider immediately, using your IMEI number, to enable your service provider to block your cell phone and your account details. Preserve all the details of launched complaints, that is, obtain confirmation in writing from your service provider that your phone has been disabled.

Box 3.6 \ Tips to Secure your . . . (Continued)

4. In case of loss of your cell phone, register a complaint at the police station and obtain FIR. Preserve all the details for launched complaints, that is, FIR report.
5. Keep an eye on your phone while traveling. During the security check at the airport security, ensure to retrieve your cell phone immediately once it enters the x-ray machine – criminals often steal phones during these vulnerable seconds.
6. Keep Wi-Fi and Bluetooth OFF when it is not required to be in use. Airports, coffee shops, hotels and all other public places wherever free Wi-Fi zone is available, criminals always have an eye to seek the vulnerability to steal information.
7. Periodic backup is important and especially if you are traveling, backup before traveling is necessary. It takes only few minutes to take backup but it is always helpful in case you lose your cell phone during traveling.
8. Do not forget to apply all the updates for cell phone software/firmware, received from manufacturers, which are routinely provided to update vulnerabilities fixes.
9. Only download applications from reputable sources – specific care should be taken while downloading plug-in applications on the cell phone. It is always advised to use the recommendations provided by cell phone manufacturers' to download directly from the Web.

Install antitheft software on your cell phone

Antitheft software does not allow the criminal to use another SIM card in the stolen cell phone. When a SIM card is changed, the system asks for a verification code. Even if the criminal manages to break this code, the phone sends out a message regarding the change of SIM to two selected contacts from the cell phone contact directory with the new SIM number. So, it becomes easy to trace the address of the new cell phone number from the service provider and thus to trace the cell. Only the owners of the cell phone will know about the installed antitheft software, as it does not show any icons on the menu. Following are few antitheft software(s) available in the market:

1. **GadgetTrak:** <http://www.gadgettrak.com/products/mobile/>
2. **Back2u:** <http://www.bak2u.com/phonebakmobilephone.php>
3. **WaveSecure:** <https://www.wavesecure.com/>
4. **F-Secure:** <http://www.f-secure.com/>

Source: <http://www.wikihow.com/Protect-a-Mobile-Phone-from-Being-Stolen>

new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones. Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

The following factors contribute for outbreaks on mobile devices:

1. **Enough target terminals:** The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization “Ojam” had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.
2. **Enough functionality:** Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.
3. **Enough connectivity:** Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

3.8.2 Mobile Viruses

A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it. Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays. In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified. First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.

Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS. Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones (i.e., if Bluetooth is always ENABLED into a mobile phone) whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book. Readers may visit <http://symbianpoint.com/types-latest-list-mobile-viruses.html> to know the list of latest mobile viruses (few viruses have been discussed in Section 3.3 Trends in Mobility).

It is interesting to note that, like Computer Virus Hoax, variants of Mobile Phone Virus Hoax^[13] have been circulating since 1999. These hoax messages either will be sent through E-Mail or through SMS to the mobile users. The example of such hoax is given.

"All mobile users pay attention!!!!!!!"

If you receive a phone call and your mobile phone displays (XALAN) on the screen don't answer the call, END THE CALL IMMEDIATELY, if you answer the call, your phone will be infected by a virus. This virus WILL ERASE all IMEI and IMSI information from both your phone and your SIM card, which will make your phone unable to connect with the telephone network. You will have to buy a new phone. This information has been confirmed by both Motorola and Nokia. There are over 3 Million mobile phones being infected by this virus in all around the world now. You can also check this news in the CNN website.

PLEASE FORWARD THIS PIECE OF INFORMATION TO ALL YOUR FRIENDS HAVING A MOBILE PHONE."

How to Protect from Mobile Malwares Attacks

Following are some tips to protect mobile from mobile malware attacks^[14]:

1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

3.8.3 Mishing

Mishing is a combination of mobile phone and Phishing (we will address this in Chapter 5). Mishing attacks are attempted using mobile phone technology. M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam. A typical Mishing attacker uses call termed as *Vishing* or message (SMS) known as *Smishing*. Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details. Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

3.8.4 Vishing

Vishing is the criminal practice of using social engineering (refer to Section 2.3 in Chapter 2) over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V – voice and Phishing (we will address Phishing in detail under Chapter 5). Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.^[15] (We will address ID Theft in detail in Chapter 5.)

The most profitable uses of the information gained through a Vishing attack include:

1. ID theft;
2. purchasing luxury goods and services;
3. transferring money/funds;
4. monitoring the victims' bank accounts;
5. making applications for loans and credit cards.

How Vishing Works

The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

1. **Internet E-Mail:** It is also called Phishing mail (we will address this in Chapter 5).
2. **Mobile text messaging:** Refer to Smishing explained in Section 3.8.5.
3. **Voicemail:** Here, victim is forced to call on the provided phone number, once he/she listens to voicemail.
4. **Direct phone call:** Following are the steps detailing on how direct phone call works:
 - The criminal gathers cell/mobile phone numbers located in a particular region and/or steals cell/mobile phone numbers after accessing legitimate voice messaging company.
 - The criminal often uses a war dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.
 - When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity. The message instructs the victim to call one phone number immediately. The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.
 - When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
 - Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
 - Such calls are often used to harvest additional details such as date of birth, credit card expiration date, etc.

Some of the examples of vished calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:

1. **Automated message:** Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options.
 - Press 1 if you need to check your banking details and live balance.
 - Press 2 if you wish to transfer funds.
 - Press 3 to unlock your online profile.
 - Press 0 for any other query.

2. Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself: "The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key."
3. The victim enters his/her bank account number and hears the next prompt: "Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950."
4. The caller enters his/her date of birth and again receives a prompt from the automated system: "Thank you. Now please type your PIN, followed by the pound key."
5. The caller enters his PIN and hears one last prompt from the system: "Thank you. We will now transfer you to the appropriate representative."

At this stage, the phone call gets disconnected, and the victim thinks there was something wrong with the telephone line; or visher may redirect the victim to the real customer service line, and the victim will not be able to know at all that his authentication was appropriated by the visher.

How to Protect from Vishing Attacks

Following are some tips to protect oneself from Vishing attacks^[16]:

1. Be suspicious about all unknown callers.
2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company – caller ID Spoofing is easy.
3. Be aware and ask questions, in case someone is asking for your personal or financial information.
4. Call them back. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.
5. Report incidents: Report Vishing calls to the nearest cyberpolice cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

3.8.5 Smishing

Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "SMS PHISHING." SMS – Short Message Service – is the text messages communication component dominantly used into mobile phones. Refer to Box 3.7 to know how SMS can be abused by using different methods and techniques other than information gathering under cybercrime.

Box 3.7 Pretexting, Sexting and VoIP Spam

Pretexting

It is also a form of social engineering, wherein a pretester hides his/her purpose and/or identity to get the personal information/sensitive data about another individual. For example, the pretester may claim his/her affiliation with a survey agency, financial institute or bank. Usually, victims are targeted over the phone and enticed to reveal their information or perform an action. It is more than a simple lie as it most often involves some prior research or setup and the use of pieces of known information (e.g., for impersonation: date of birth, pet names of family members and last bill amount) to establish legitimacy in the mind of the target.^[17]

This technique is often used to trick the executives to disclose the information about their customer and/or their competitor and is used by private investigators to obtain telephone records, banking

Box 3.7 Pretexting, . . . (Continued)

records, utility records and other information directly from junior representatives of an organization. However, nowadays, this technique is also used by the criminals through Vishing and Smishing attacks.

Sexting

It is the practice of sending sexually explicit text messages and photos over the cell phone. It is becoming an increasingly hot topic both in schools/colleges and in the workplace. Although most of the people think instantly of cell phones as sexting devices, digital photography, Internet (i.e., websites) and even few video game systems are also contributing sexting.^[18]

Sexting is a complex topic and no one-size-fits-all solution is available, reason being that it embraces everything from gentle naughty-blue pictures to slimy pornography. Many teens (especially, girls) who believe they are sending a private message, may have their messages widely distributed, sometimes even immediately available on porno sites. So, it is important that parents should keep an eye on the cell phones provided to the kids. Kids should be made aware that “*Information shared electronically never dies*” and any message such as sexting may come back to haunt them even after months and years.

VoIP Spam

VoIP Spam is the proliferation of unwanted, automatically dialed and prerecorded phone calls using VoIP. Some pundits have taken to referring to it as “Spam over Internet telephony” (SPIT).^[19] VoIP systems, such as E-Mail and other Internet applications, are susceptible to abuse by criminals to initiate unsolicited and unwanted communications. Increasingly, telemarketers, prank callers and other telephone system abusers are likely to target VoIP systems, particularly, if VoIP tends to supplant conventional telephony.

Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. The popular technique to “hook” (method used to actually “capture” your information) the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI.

Smishing works in the similar pattern as Vishing. A few examples of Smishing are provided herewith to demonstrate how the victim is forced to disclose PI.

1. “We are happy to send our confirmation toward your enrolment for our ‘xxxxxxxx Club Membership.’ You will be charged ₹ 50/- per day, unless you reconfirm your acceptance of your membership on our “Membership Office Contact no. XXXXXXXXXXXX.”
2. “[Name of popular online bank] is confirming that you have purchased LCD TV set, worth of ₹ 90,000/- only from (name of popular computer company)]. Visit www.abcdef.com if you did not make this online purchase.”

How to Protect from Smishing Attacks

Following are some tips to protect oneself from Smishing attacks:

1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.

Box 3.8 SMS Blocker

India-based organization Optinno Mobitech Pvt. Ltd. has innovated and launched an application, *smsBlocker*, which runs on mobile phones and ensures 100% Spam blockage. *smsBlocker* is powered with a unique intuitive algorithm to detect and block Spam SMS automatically. However, mobile user can also customize the filtering levels as per his/her own privacy requirements. *smsBlocker* is configured to the unique mobile handset identification number, that is, IMEI. Thus, if a mobile user changes the mobile handset, *smsBlocker* will not work on the new mobile handset; however, if SIM card is changed it will not affect *smsBlocker*. *smsBlocker* is designed for all mobile handsets that support Symbian OS. It is interesting to note that *smsBlocker* does not require GPRS/Internet connection.

Source: <http://www.smsblocker.in> (30 July 2010).

3. Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites. Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

3.8.6 Hacking Bluetooth

Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile devices (see Box 3.9). Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication. The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.

When Bluetooth is enabled on a device, it essentially broadcasts “I’m here, and I’m able to connect” to any other Bluetooth-based device within range. This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers. The attacker installs special software [see Table 3.1 for list of software(s) which are termed as *Bluetooth hacking tools*] on a laptop and then installs a Bluetooth antenna. Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

Box 3.9 Bluetooth

The word Bluetooth is an anglicized form of Danish *Blåtand* – Harald Bluetooth was king of Denmark in the 10th century, who managed to unite Denmark and parts of Norway into a single kingdom. The king was killed in 986 AD during a battle with his son. Choosing this name indicates how important companies from the Nordic region (nations including Denmark, Sweden, Norway and Finland) are to the communications industry, even if this name says little about the way the technology works. The implication is that Bluetooth does the same with communication protocols, uniting them into one universal standard. *blå* in modern Scandinavian languages means blue and (historically) correct translation of Old Norse *Harald Blátönn* could be Harald Bluetooth.

The Bluetooth logo is a bind rune merging the Germanic runes  (Hagall) and  (Berkana).

Table 3.1 | Bluetooth hacking tools

Sr. No.	Name of the Tool	Description
1	BlueScanner	This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2	BlueSniff	This is a GUI-based utility for finding discoverable and hidden Bluetooth-enabled devices.
3	BlueBugger	The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4	Bluesnarfer	If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5	BlueDiving	Bluediving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.

- Bluejacking:** It means *Bluetooth + Jacking* where Jacking is short name for *hijack* – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius), for example, sending a visiting card which will contain a message in the name field. If the user does not recognize/realize what the message is, he/she might allow the contact to be added to her/his address book, and the contact can send him messages that might be automatically opened because they are coming from a known contact. Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.
- Bluesnarfing:** It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.
- Bluebugging:** It allows attackers to remotely access a user's phone and use its features without user's attention. During initial days, the attacker could simply listen to any conversation his/her victim is having; however, further developments in Bluebugging tools have enabled the attacker with the ability to take control of the victim's phone and to conduct many more activities such as initiate phone calls; send and read SMS; read and write phonebook contacts; eavesdrop on phone conversations and connect to the Internet.
- Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo. Further research is underway to know whether Bluetooth attackers could do anything more serious such as disabling airbags or brakes through this kind of attack. The researchers are also investigating about possibility of an attacker accessing a telephone address book once the connection gets established with the Bluetooth system through this kind of attack.

Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking. These vulnerabilities are an inevitable result of technological innovation, and device manufacturers' continuously research and release firmware upgrades to address new challenges/problems as they arise.

Box 3.10 Hacking Mobile Phones

Chris Paget, a hacker, conducted a demonstration on how to intercept mobile phone calls using an equipment that costs not more than US\$ 1,500, at a DefCon conference in Las Vegas.

The hacker used a simple antenna and some basic radio equipments to broadcast a GSM signal and pretend to be a telecom service provider. After this clever trick, it is possible for a hacker to forward his/her own calls and listen to any conversation that takes place within the network.

Although this demonstration is limited to GSM networks, the hacker is quite confident about causing disruption into 3G mobile networks with a simple noise generator and a power amplifier.

Smart readers can immediately conclude that although INTEGRITY is always challenged during the transmitting of the text messages, the threat of breaching the voice communication has also become important under cybersecurity.

Source: <http://www.geekwithlaptop.com/hacker-demonstrates-powerful-mobile-interception-at-minimal-expense> (3 August 2010).



"Bluetooth and Bluetooth Security" is a separate subject in itself. Readers may visit the following websites to explore more on this topic:

- <https://www.bluetooth.org/apps/content/>
- <http://www.bluetooth.com/English/Pages/default.aspx>
- <http://www.bluetoothhack.info/>

3.9 Mobile Devices: Security Implications for Organizations

3.9.1 Managing Diversity and Proliferation of Hand-Held Devices

In the previous sections we have talked about the microissues of purely technical nature in mobile device security. In this section, we focus on the macroissues at the organizational level. Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their security objectives, subject to legal and other external constraints. Some organizations will implement security procedures and tools extensively, whereas others will place more value on cost and convenience. Whatever approaches an organization chooses, it is important that the policy-making effort starts with the commitment from a Chief Executive Officer (CEO), President or Director who takes cybersecurity seriously and communicates that throughout an organization. The best security technology features will be found to be worthless if there is no organization policy or automated enforcement to ensure that they are actually used.

In some cases, for example, senior executives have been given special access rights to the corporate network which can circumvent standard security procedures. Cybersecurity is always a primary concern; even then, at times, there is still some short sightedness. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered in corporate asset register irrespective of whether or not the devices have been provided by the organization. In addition (recall the microlevel technical issues discussed in the previous section), close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove his/her logical as well as physical access to corporate resources because employees (for malicious or other reasons) could be using their mobile devices to connect into the corporate networks. Thus, mobile devices that belong to the company should be returned to the IT department and, at the very least, should be deactivated and cleansed.

Box 3.11**TrustZone Technology for Mobile Devices – Toward Security of M-Commerce Applications**

About 2 years back, Trusted Logic Security Module was announced for Microsoft Windows CE 5.0. With this, developers of Windows CE 5.0 can use Trusted Logic software to increase electronic transaction security in ARM-powered(R) devices, which is very pertinent in the M-Commerce paradigm.

The Windows CE 5.0 evaluation version of the security module, coupled with the ARM TrustZone technology, provides consumers with a more secure environment for electronic transactions such as M-Banking, E-Commerce and digital rights management (DRM) (refer to Appendix N). This security can be designed into ARM-powered consumer devices such as mobile phones, payment terminals and set-top boxes.

The security module implements the TrustZone APIs to enable smooth evolution and compatibility with future versions of the software running on ARM TrustZone technology-enabled processors. The software is part of a portfolio of embedded security products offered by ARM and developed under a recently announced agreement between Trusted Logic and ARM.

ARM TrustZone architecture extensions build security into the processor itself whereas TrustZone software provides trusted foundation software, protected by the hardware, enabling OS providers, handset vendors and silicon designers to expand and develop their own security solutions on top of an interoperable framework. Currently, security-aware applications must be rewritten for every security platform they run on. However, the new TrustZone Software API provides a standard interface for these applications to be partitioned and to communicate with a secure-side component independent of the actual system implementation.

According to experts, M-Commerce applications can now target multiple security platforms and speed up the development. Industry analysts say that this is a technical collaboration between Microsoft and ARM. This is being considered as a good step toward making mobile devices more secure and is critical to the success of next-generation mobile applications.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

In addition, employees should be encouraged to register with the IT department any devices they use for themselves, so that access can be provisioned in a controlled manner and de-provisioned appropriately when the employee leaves.

Younger workers (also referred to as Gen-Y) are pushing many enterprises to embrace mobility solutions. These younger workers prefer instant/text messaging instead of E-Mail, and frequently use social networking services such as Facebook, MySpace and Twitter. They often prefer to use personal, consumer-oriented devices (both laptops and mobile devices) in the work environment, and adapt quickly to new technology. In contrast, older workers are found to be slow to accept mobility solutions and rely almost entirely on voice communications and E-Mail. These old workers often do not see the benefit of instant messaging and social networking. Interestingly, at the same time these older workers are often found to be on the seat that provides authority and control for staffing and budget, and they can therefore greatly influence mobility policy. These different points of view between younger and older workers have created a mobility generational gap. Older workers sometimes see younger workers as being “spoiled” whereas younger workers sometimes see older workers as a barrier to progress.

3.9.2 Unconventional/Stealth Storage Devices

We have already mentioned about mobile phones and media players used by the employees. In this section, we would like to emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees. As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes – unconventional/stealth storage devices available nowadays are difficult to detect and have become a

prime challenge for organizational security. It is advisable to prohibit the employees in using these devices [see Figs. 3.12(a) and (b)]. Their small size allows for easy concealment anywhere in a bag or on the body.

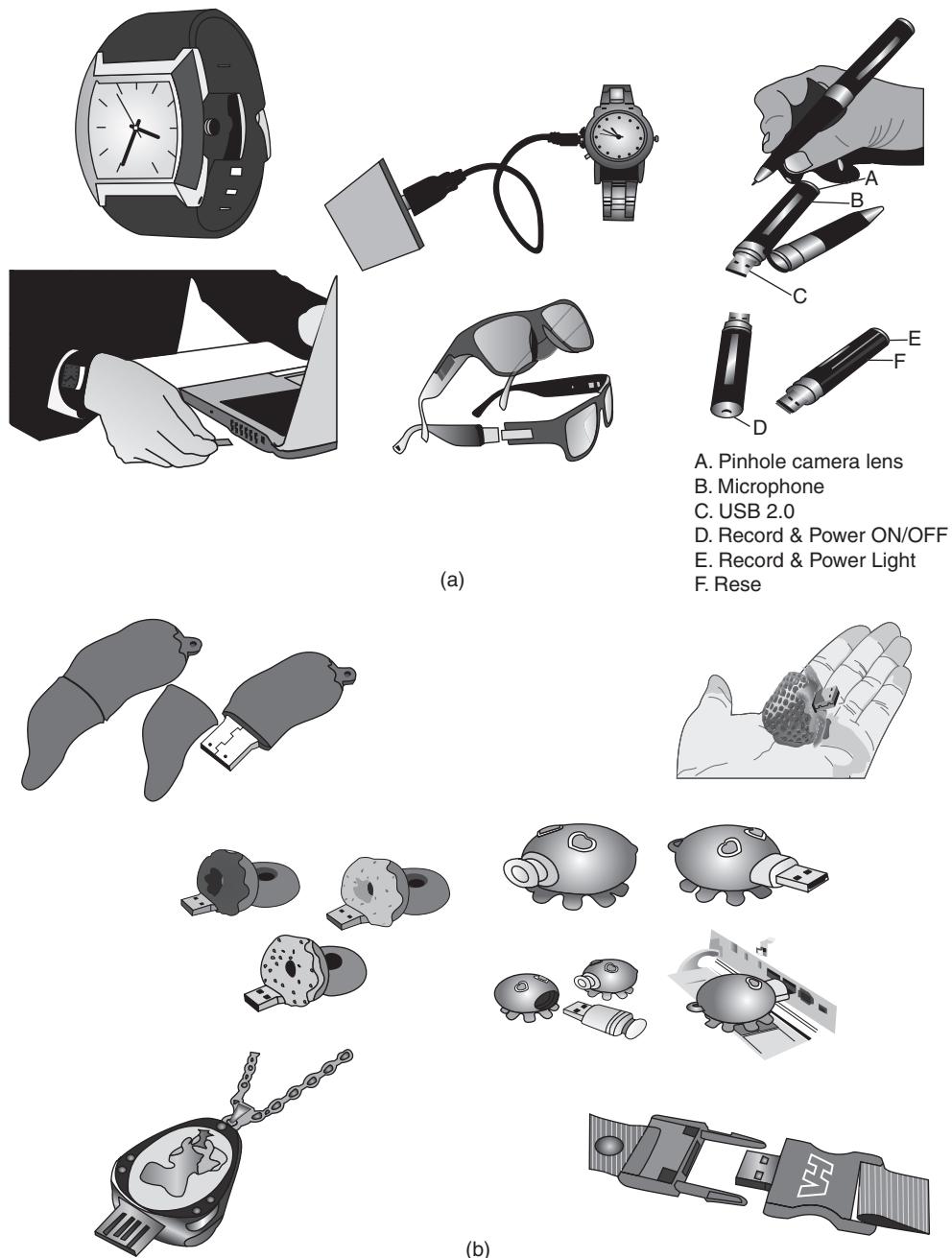


Figure 3.12 | Unconventional/stealth storage devices.

Firewalls and antivirus software are no defense against the threat of open USB ports. Not only can *viruses*, *worms* and *Trojans* (we will discuss more in Chapter 4) get into the organization network, but can also destroy valuable data in the organization network. Organization has to have a policy in place to block these ports while issuing the asset to the employee. However, sometimes the standard access controls with Windows OS do not allow the assignment of permissions for USB ports and restricting these devices becomes next to impossible. Disgruntled employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended computer and will be able to download confidential data or upload harmful viruses. As the malicious attack is launched from within the organization, firewalls and antivirus software are not alerted.

Using “DeviceLock” software solution, one can have control over unauthorized access to plug and play devices (for more details, visit <http://www.devicelock.com/>). The features of the software allows system administrator to:

1. Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.
2. Control the access to devices depending on the time of the day and day of the week.
3. Create the white list of USB devices which allows you to authorize only specific devices that will not be locked regardless of any other settings.
4. Set devices in read-only mode.
5. Protect disks from accidental or intentional formatting.

Another factor in cybersecurity complications with mobile devices is their falling cost. Until few years ago, mobile devices were considered as an office supply item instead of a powerful computing platform. Early hand-helds were *expensive* and *specialized*, so they were deployed only for specific applications, but more general-purpose models are now available at a relatively low cost, often bundled with a tariff for wireless connection. So, many organizations did not have policies concerning the usage of mobile/wireless devices at work/connected with work. Nowadays, because modern hand-held devices for mobile computing are, at times, good productivity tools, they cannot be precluded from use by employees, contractors and other business entities. Given this, it is important for the device management teams to include user awareness education; thus, they get encouraged to take some personal responsibility for the physical security of their devices, as many IT managers have learned from their bitter experience.

3.9.3 Threats through Lost and Stolen Devices

This is a new emerging issue for cybersecurity. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations. A report based on a survey of London’s 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period. Today this figure (lost mobile devices) could be far larger given the greatly increased sales and usage of mobile devices. See Box 3.12 for some interesting facts on lost mobile devices.

The cybersecurity threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the hand-held device that is important but rather the content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity, as most of the times the mobile hand-held devices are provided by the organization. Most of these lost devices have wireless access to a corporate network and have potentially very little security, making them a weak link and a major headache for security administrators. Even if these lost devices are personal, the issue is no less serious given the resulting privacy exposures! Gartner Group had predicted that by 2003 there will be over one billion mobile devices in use globally. This is true going by the sales figures quoted in annual

Box 3.12 Getting Lost!!

Cities and countries in which drivers were surveyed were Chicago; Copenhagen, Denmark; Helsinki, Finland; London; Munich, Germany; Oslo, Norway; Paris; Stockholm, Sweden and Sydney, Australia.

1. Pointsec Mobile Technologies, Inc. has discovered where lost electronic devices go: they wind up in the back seats of taxis all around the world!!
2. A survey of 935 cabbies in 9 countries turned up 85 notebook computers, 227 PDAs and 2,238 cell phones lost in cabs in the last 6 months.
3. As per Gartner 2002 report, nearly 250,000 hand-held devices were left behind in the US airports in 2002, and of those, only about 30% were traced back and returned to their owners.
4. Copenhagen appears to have the most forgetful cell phone users, with 719 phones left behind in 100 cabs in a 6-month period. Chicago cab riders left behind 387 in the same period. In total, 97 PDAs and 20 notebooks were reported lost in Chicago. London cabbies reported 23 laptops left behind.
5. As per Gartner 2004 study, a company with 5,000 or more employees could save US\$ 300,000–500,000 annually by tagging, tracking and recovering mobile phones and PDAs.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

reports published by Research in Motion. This shows that the popularity of mobile devices is increasing at a rapid rate; however, people have not been educated about the importance of securing them. The picture is indeed scary; mobile users are in an even worse position now because they are far more reliant on their mobile devices to store large amounts of sensitive information with very few concerned about backing it up or protecting it.

3.9.4 Protecting Data on Lost Devices

Given the above discussion, readers can appreciate the importance of data protection especially when it resides on a mobile hand-held device. At an individual level, employees need to worry about this. There are two reasons why cybersecurity needs to address this issue: data that are persistently stored on the device and always running applications. For protecting data that are stored persistently on a device, there are two precautions that individuals can take to prevent disclosure of the data stored on a mobile device: (a) encrypting sensitive data and (b) encrypting the entire file system (this may be useful when using data outside of a database, such as in a spreadsheet). Data that are stored on hard disks in persistent memory or on removable memory sticks (whether they are in or out of the device) should be protected. There are many third-party solutions/tools available to protect data on the lost devices, including encrypting the servers where a database file is residing. There are solutions using which individuals can enforce a self-destruct policy to destroy privileged data on a lost device or create a database action to delete the data on a user's device using a suitable tool.

A key point here is that the organizations should have a clear policy on how to respond to the loss or theft of a device, whether it is data storage, a PDA or a laptop. There should be a method for the device owner to quickly report the loss, and device owners should be aware of this method. Writing the emergency contact information on the device itself is unlikely to be very helpful.

3.9.5 Educating the Laptop Users

Often it so happens that corporate laptop users could be putting their company's networks at risk by downloading non-work-related software capable of spreading viruses and Spyware. This is because the software

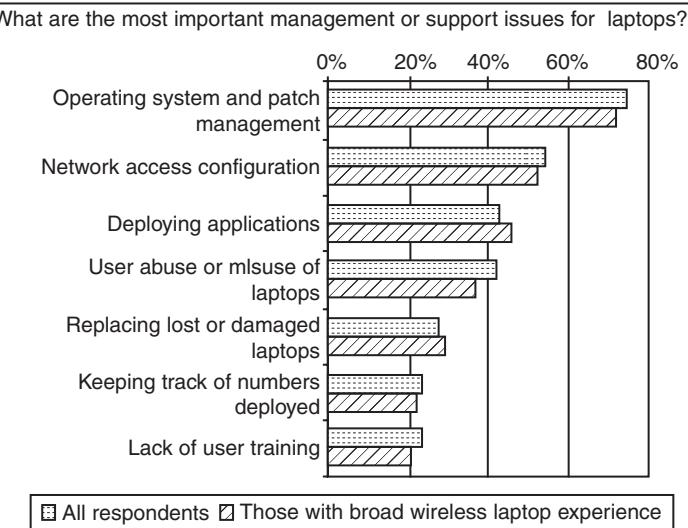


Figure 3.13 Most important management or support issues for laptops.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

assets on laptops become more complex as more applications are used on an increasingly sophisticated OS with diverse connectivity options.

According to year 2004 finding, through one survey, it was found that some 86% of employees with laptops admitted to installing software onto their machines when outside of the office, with many using their laptops to access peer-to-peer websites and downloading illegal music files and movies. As per one survey of 500 European business laptop users, Malicious Code, such as Spyware and viruses, is infecting laptops and consequently business networks when they are reconnected to the corporate systems.

The result from a survey quoted in Fig. 3.13 further supports this point on cybersecurity threats from corporate laptop users. However, despite the growth in corporate security risks, resulting from mobile working, the tone of most of the security-awareness surveys shows that only half of the companies have tools in place to manage the Internet access on laptops, with only one-quarter of businesses physically enforcing these policies. An important point to be noted is that the policies and procedures put in place for support of laptop have evolved over the years to be able to cope successfully with managing laptops, connected by wireless means or otherwise. This shows how much role “perception” plays in terms of most people perceiving laptops as greater culprits compared with other innocuous-looking mobile hand-held devices.

3.10 Organizational Measures for Handling Mobile Devices-Related Security Issues

So far, we have discussed micro- and macrolevel security issues with mobile devices used for mobile computing purposes and what individuals can do to protect their personal data on mobile devices. In this section, we discuss what organizations can do toward safeguarding their information systems in the mobile computing paradigm.

3.10.1 Encrypting Organizational Databases

Critical and sensitive data reside on databases [say, applications such as customer relationship management (CRM) that utilize patterns discovered through *data warehousing* and *data mining* (DM) techniques] and with the advances in technology, access to these data is not impossible through hand-held devices. It is clear that to protect the organizations' data loss, such databases need encryption. We mention here two algorithms that are typically used to implement strong encryption of database files: Rijndael (pronounced rain-dahl or Rhine-doll), a block encryption algorithm, chosen as the new Advanced Encryption Standard (AES) for block ciphers by the National Institute of Standards and Technology (NIST). (See Ref. #13, Additional Useful Web References, Further Reading). The other algorithm used to implement strong encryption of database files is the Multi-Dimensional Space Rotation (MDSR) algorithm developed by Casio.

The term "strong encryption" is used here to describe these technologies in contrast to the simple encryption. *Strong encryption* means that it is much harder to break, but it also has a significant impact on performance. Database file encryption technology, using either the AES or the MDSR algorithms, makes the database file inoperable without the key (password). Encrypting the database scrambles the information contained in the main database file (i.e., all temporary files and all transaction log files) so that it cannot be deciphered by looking at the files using a disk utility. There is a performance impact for using strong encryption. A weaker form of encryption is also available that has negligible performance impact.

When using strong encryption, it is important *not* to store the key on the mobile device: this is equivalent to leaving a key in a locked door. However, if you lose the key, your data are completely inaccessible. The key is case-sensitive and must be entered correctly to access your database. The key is required whenever you want to start the database or you want to use a utility on your database. For greater security there is an option available that instructs the database server to display a dialog box where the user can enter the encryption key. This option is necessary because the encryption key should not be entered on the machine in clear text. To protect the scenario of information attack/stealing through the mobile devices connecting to corporate databases, additional security measures are possible through enforcing a self-destruct policy that is controlled from the server. When a device that is identified as lost or stolen connects to the organization server, IT department can have the server send a package to destroy privileged data on the device.

3.10.2 Including Mobile Devices in Security Strategy

The discussion so far makes a strong business case – in recognition of the fact that our mobile workforce is on the rise, organizational IT departments will have to take the accountability for cybersecurity threats that come through inappropriate access to organizational data from mobile-device–user employees. Encryption of corporate databases is not the end of everything. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse, saying they fear the loss of sensitive data that could result from a PDA being stolen or an unsecured wireless connection being used. Their concerns are no longer viable. There are technologies available to properly secure mobile devices. These should be good enough for most organizations. Corporate IT departments just need to do their homework. For example, there are ways to make devices lock or destroy the lost data by sending the machine a special message. Also, some mobile devices have high-powered processors that will support 128-bit encryption. Although mobile devices do pose unique challenges from a cybersecurity perspective, there are some general steps that the users can take to address them, such as integrating security programs for mobile and wireless systems into the overall security blueprint. A few things that enterprises can use are:

1. Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.

2. Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.
3. Develop a system of more frequent and thorough security audits for mobile devices.
4. Incorporate security awareness into your mobile training and support programs so that everyone understands just how important an issue security is within a company's overall IT strategy.
5. Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

In the next section, our focus is on security policies relating to mobile devices.

3.11 Organizational Security Policies and Measures in Mobile Computing Era

3.11.1 Importance of Security Policies relating to Mobile Computing Devices

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People (especially, the youth) have grown so used to their hand-holds that they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their hand-held devices (we have already discussed the threats through media player when we talked about microlevel technical issues for cybersecurity threats through these devices). One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information. Not only would this be a public relations (PR) disaster, but it could also violate laws and regulations. One should give a deep thought about the potential legal troubles for a public company whose sales reports, employee records or expansion plans may fall into wrong hands.

When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure. This sort of policy can be difficult to enforce, however, by increasing awareness of the user, it can be reasonably effective. Information classification and handling policy should clearly define what sorts of data may be stored on mobile devices. In the absence of other controls, simply not storing confidential data on at-risk platforms will mitigate the risk of theft or loss.

A survey^[20] released by the Ponemon Institute, on behalf of Cellcrypt (www.cellcrypt.com), reveals that large and medium businesses are putting themselves at risk as a result of cell phone voice call interception. According to this survey of 75 companies and 107 senior executives in the US, it costs US corporations on average US\$ 1.3 million each time a corporate secret is revealed to unauthorized parties. About 18% of respondents estimate such losses to occur weekly or more frequently, 61% at least monthly and 90% at least annually.

The survey asked the participants about the likelihood of six separate scenarios involving the use of cell phones to communicate sensitive and confidential information occurring in their organizations. The scenarios described the following:

1. A CEO's administrative assistant uses a cell phone to arrange ground transportation that reveals the CEO's identity and location.

2. The finance and accounting staff discusses earnings of press release and one participant on the call is using a cell phone.
3. A conference call among senior leaders in the organization in which cell phones are sometimes used.
4. A sales manager conducting business in Asia uses, his/her cell phone to communicate with the home office.
5. An external lawyer asks for proprietary and confidential information while using his cell phone.
6. A call center employee assists a customer using a cell phone to establish an account and collects personal information (including SSN).

3.11.2 Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.
2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques (retinal scans, iris scans, etc.) can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
4. Develop a specific framework for using mobile computing devices, including guidelines for data-syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized inventory database.
7. Label the devices and register them with a suitable service that helps return recovered devices to the owners.
8. Establish procedures to disable remote access for any mobile devices reported as lost or stolen. Many devices allow the users to store usernames and passwords for website portals, which could allow a thief to access even more information than on the device itself.
9. Remove data from computing devices that are not in use or before re-assigning those devices to new owners (in case of company-provided mobile devices to employees). This is to preclude incidents through which people obtain “old” computing devices that still had confidential company data.
10. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

3.11.3 Organizational Policies for the Use of Mobile Hand-Held Devices

The first step in securing mobile devices is creating company policies that address the unique issues these devices raise. Such questions include what an employee should do if a device is lost or stolen. We have talked about this in Section 3.9.4.

There are many ways to handle the matter of creating policy for mobile devices. One way is creating a distinct mobile computing policy. Another way is including such devices under existing policy. There are also approaches in between, where mobile devices fall under both existing general policies and a new one. In the hybrid approach, a new policy is created to address the specific needs of the mobile devices (such as what to do if they are lost or stolen) but more general usage issues fall under general IT policies. As a part of this approach, the “acceptable use” policy for other technologies is extended to the mobile devices. There may not be a need for separate policies for wireless, LAN, wide area network (WAN), etc. because a properly written network policy can cover all connections to the company data, including mobile and wireless.

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time that they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices. For example, wireless devices pose different challenges than non-wireless devices. Also, employees who use mobile devices more than 20% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs.

It is never too early to start planning for mobile devices, even when a company, at a given point of time, cannot afford creating any special security policies to mitigate the threats posed by mobile computing devices to cyber-security. It is, after all, an issue of new technology adoption for many organizations. By contemplating its uses, companies may think of ways they can use it and, perhaps just as important, how their competitors will use it.

3.12 Laptops

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable.

Box 3.13 Spy Phone Software!!!

Spy Phone software is installed on the mobile/cell phone of employees, if the employers wants to monitor phone usage. The Spy Phone software is completely hidden from the user, once it is installed and collects all the available data such as SMS messages, incoming/outgoing call history, location tracking, GPRS usage and uploads the collected data to a remote server.

The employer can simply access the designated website hosted by Spy Phone vendor, and after entering his/her account details, he/she can have full access to all the data collected 24 hours a day, 7 days a week. The employer can access this website through the Internet; hence, he/she can keep an eye on their employees, regardless where he/she is in the world. The employer can read all SMS messages (both incoming and outgoing), know who they (employees) are calling or who is calling them and where they were when the call was received.

Following are few Spy Phone Software(s) available in the market:

1. **SpyPhonePlus:** <http://www.spyphoneplus.com/>
2. **FlexiSpy:** <http://www.flexispy.com/>
3. **TheSpyPhone:** <http://www.thespyphone.com/spyphone.html>
4. **Mobile Spy:** <http://www.mobile-spy.com/>

Wireless capability in these devices has also raised cybersecurity concerns owing to the information being transmitted over other, which makes it hard to detect. In this section, we provide an elaborate discussion as to what measures the organizations can take in the face of cybersecurity threat brought by the widespread use of laptops.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive.

Such information can be misused if found by a malicious user. Senior executives commonly believe that the information stored on their laptops is only useful for them and would not be of any interest to others. Owing to this belief, most senior executives in an organization feel that it is unnecessary to protect the information stored on these laptops. However, this is not true. The following section provides some countermeasures against the theft of laptops, thereby avoiding cybersecurity exposures.

3.12.1 Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees' laptops and to reduce the likelihood that employees will lose laptops. Management also has to take care of creating awareness among the employees about physical security countermeasures by continuous training and stringent monitoring of organizational policies and procedures about these physical security countermeasures.^[21]

1. **Cables and hardwired locks:** The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cables [see Figs. 3.14 (a) and (b)]. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms. However, the downside of the security cables lies in the fact that one can easily remove detachable bays such as CD-ROM bay, Personal Computer Memory Card Industry Association (PCMCIA) cards (see Ref. #10, Additional Useful Web References, Further Reading), hard disk drive (HDD) bay and other removable devices from the laptop as the cable only secures the laptop from being stolen. The other disadvantage of security cables is when the laptop is locked to an object that is not fixed or is weak enough for anyone to break it. In certain cases of laptop thefts, the thief dismantled or smashed the fixed item to which the laptop was attached to.
2. **Laptop safes:** Safes made of polycarbonate – the same material that is used in bulletproof windows, police riot shields and bank security screens – can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.
3. **Motion sensors and alarms:** Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to



(a)



(b)

Figure 3.14 (a) Kensington cable locks for laptops. (b) Closer view of cable locks for laptops.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

their loud nature, they help in deterring thieves. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device that communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device and the key ring device crosses the specified range. Also available are security PCMCIA cards that act as a motion detector, an alarm system, and also have the capability to lockdown the laptop if the laptop is moved out of the designated range. They also secure the passwords and encryption keys and prevent access to the OS. These cards have batteries that keep them powered on even when the system is shutdown. Figure 3.15 shows some laptop alarm systems with sensors.

4. **Warning labels and stamps:** Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or key employees of the organizations.
5. **Other measures for protecting laptops are as follows:**
 - Engraving the laptop with personal details;
 - keeping the laptop close to oneself wherever possible;
 - carrying the laptop in a different and unobvious bag making it unobvious to potential thieves;



Figure 3.15 | Laptop alarm systems with sensors.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

- creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop;
- making a copy of the purchase receipt, laptop serial number and the description of the laptop;
- installing encryption software to protect information stored on the laptop;
- using personal firewall software to block unwanted access and intrusion;
- updating the antivirus software regularly;
- tight office security using security guards and securing the laptop by locking it down in lockers when not in use;
- never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an antitheft device;
- disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

So far, we have discussed protection of corporate laptops in terms of physical access control. However, information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/open access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handling of removable drives/storage mediums/unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls/intrusion detection system (IDSs).
10. Encrypting critical file systems.
11. Other countermeasures:
 - Choosing a secure OS that has been tested for quite some time and which has a high security incorporated into it.
 - Registering the laptop with the laptop manufacturer to track down the laptop in case of theft.
 - Disabling unnecessary user accounts and renaming the administrator account.
 - Disabling display of the last logged in username in the login dialog box.
 - Backing up data on a regular basis.

SUMMARY

Everyday mobile workers take laptop computers and hand-held devices outside of their organizations' secure environment. Cell phones, PDAs, Smartphones, laptop computers and other devices make it convenient to access information anywhere. However, the potential for confidential information to be exploited on these devices and the ability to access corporate networks from outside the firewall,

as well as the susceptibility of these devices to loss and theft, create cybersecurity risks that must be addressed in order to protect the privileged data. Therefore, in this chapter, we have discussed the nature of mobile hand-held devices and how they have the potential to create exposure to information systems security in the organizations. We have emphasized and reiterated the key point that the

widespread use of mobile devices as well as information explosion calls for a higher-level security in the mobile devices. In this chapter, we have discussed cybersecurity challenges in mobile and wireless computing scenario. The challenge here is that IT departments and security professionals need to handle this issue with due seriousness. Mobile devices such as PDAs and Smartphones have become a key tool for traveling employees to help enable their digital lives both in the office and on the road. As more employees, including executives, begin to carry such devices, the amount of sensitive and confidential information at risk increases. Although PDAs and Smartphones can greatly enhance employee productivity, they can also be easily lost or stolen. Without protection, sensitive data stored on mobile devices may be breached, potentially resulting in damages, including lost revenue, regulatory penalties and loss of brand reputation and goodwill of the business enterprise. We have seen the different

kinds of attacks launched on the mobile/cell phones by criminals and also some tips to avoid being victims of such attacks. Thus, the key point is that as mobile technology becomes ubiquitous, mobile security becomes increasingly important. Within a decade, mobile devices (PDAs, cell phones, wrist-watches, etc.) will function as wallets, electronic banks (E-Banks), business cards, proximity keys, as well as the personal information managers (PIMs) and communicators they are today.

Our final key point in this chapter is that protecting the data on a device is just as important as protecting the information flowing between the device and the servers it interacts with. Device security is often something that is left up to the end-user to implement and maintain. Although this is often driven by corporate policy, enterprises often look for ways to take this responsibility out of the hands of end-users and place it under the enforceable control of an administrator.

REVIEW QUESTIONS

1. What are the “mobility types”? Quote day-to-day examples of your familiarity that relates to them.
2. Discuss how “perception” makes people least suspect cybersecurity threats through mobile computing hand-held devices. What measures do you recommend against this situation?
3. What kinds of attacks are possible on mobile/cell phones? Explain with examples.
4. Explain the countermeasures to be practiced for possible attacks on mobile/cell phones.
5. What kinds of cybersecurity measures an organization should have to take in case of portable storage devices? Prepare security guidelines which can be implemented in an organization.
6. Explain the various measures for protection of laptops through physical measures and logical access control measures. Prepare a laptop security checklist using the guidelines provided in this chapter. Apply it to the laptop owner in your educational institute. If you are employed, then find out your organization’s laptop protection policy and related procedures.

REFERENCES

- [1] Quocirca Insight Report (2009), *Addressing a Growing Problem: An Explosion of IP Addresses*, visit: <http://www.quocirca.com> (31 March 2010).
- [2] Research In Motion Inc., *Research in Motion Annual Report*, 2009, visit: http://www.rim.com/investors/pdf/RIM09AR_FINAL.pdf (21 March 2006).
- [3] To know more about mobile computing and types of mobile computing, visit: http://en.wikipedia.org/wiki/Mobile_computing (28 March 2010).

- [4] To know more on *Mobile Security – Problem in Hand, Solution in Mind*, visit: http://www.it-analysis.com/blogs/Quocirca/2009/4/mobile_security_problem_in_hand_so_.html (31 March 2010).
- [5] Quocirca Insight Report (2005), *Mobile Devices and Users*, visit: <http://www.quocirca.com> (15 May 2010).
- [6] To know more about “3G Mobile Networks – Security Concerns,” visit: <http://fanaticmedia.com/infosecurity/archive/April09/3G%20Mobile%20Networks.htm> (10 April 2010).
- [7] To learn about credit card transactions using mobile cell phone, visit: <https://www.frontlineprocessing.com/news/wireless-credit-card-processing/> (15 May 2010).
- [8] To know how to avoid credit and charge card fraud, visit: <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre07.shtm> (24 February 2010).
- [9] CLEW Technology (*Closed-Loop Environment for Wireless*) comes from Alacrity, an Australian company who specifically created to deliver on the promise of mobile Internet. Alacrity’s patented CLEW technology provides instant interactivity with their clients for time critical information. For further details, visit: <http://www.alacritytech.com.au> (15 May 2010).
- [10] To know more about Types of Credit Card Fraud, visit:
<http://people.exeter.ac.uk/watupman/undergrad/owsylves/page3.html> (22 May 2010).
http://en.wikipedia.org/wiki/Credit_card_fraud (22 May 2010).
- [11] For a news item *Microsoft Paves over Media Player Flaws*, visit: <http://news.com.com/2100-1023-940050.html> (19 May 2003).
- [12] To know how to protect a mobile phone from being stolen, visit: <http://www.wikihow.com/> Protect-a-Mobile-Phone-from-Being-Stolen (20 February 2010).
- [13] To know more about Mobile Phone Virus Hoax, visit: <http://www.hoax-slayer.com/mobile-phone-virus-hoax.html> (22 May 2010).
- [14] To know more about Help protect against mobile viruses, visit: <http://www.microsoft.com/uk/protect/computer/viruses/mobile.mspx> (22 May 2010).
- [15] To know more about Vishing, visit: <http://en.wikipedia.org/wiki/Vishing> (20 February 2010).
- [16] To know more about how to protect from Vishing attacks, visit: http://news.cnet.com/8301-1035_3-10244200-94.html (18 February 2009).
- [17] To know more about pretexting, visit: [http://en.wikipedia.org/wiki/Social_engineering_\(security\)](http://en.wikipedia.org/wiki/Social_engineering_(security)) (18 February 2009).
- [18] To know more about sexting, visit: <http://en.wikipedia.org/wiki/Sexting> (18 February 2009).
- [19] To know more about VoIP spam, visit: http://en.wikipedia.org/wiki/VoIP_spam (18 February 2009).
- [20] To know more about US Businesses Losing Millions from Illegal Interception of cell phone calls, visit:
<http://www.darkreading.com/insiderthreat/security/perimeter/showArticle.jhtml?articleID=223101287> (22 May 2010).
http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100302006258&newsLang=en (22 May 2010).
- [21] To know more about Laptop Security, visit: <http://www.securitydocs.com/pdf/3399.PDF> (22 May 2010)

FURTHER READING

Additional Useful Web References

1. Alexander, Z. (1997) *Is RAS Safe?*, WindowsITPro magazine – <http://www.windowsitpro.com/article/networking/optimizing-nt-ras.aspx> (15 May 2010).

2. To see interesting information in the article *Protecting your Laptop Computer*, visit: http://itso.iu.edu/Protecting_Your_Laptop_Computer (15 May 2010).

3. For *Windows Media Player Control Registry Settings*, visit: <http://msdn.microsoft.com/en-us/library/ms909920.aspx> (15 May 2010).
 4. To study the projects done by the *Security Research Group*, visit: <http://research.microsoft.com/en-us/groups/security/> (15 May 2010).
 5. For another similar news item titled *Real Networks Warns of Media Player Security Flaws*, visit: <http://www.networkworld.com/news/2004/0206realwarns.html> (15 May 2010).
 6. For a very informative article on secure operation of the RAS system, visit: <http://www.iwar.org.uk/comsec/resources/standards/germany/itbpms/s4112.htm> (15 May 2010).
 7. For an interesting article titled *Butter-Fingered Mobile Device Users create IT Risk*, visit: <http://www.networkworld.com/newsletters/wireless/2005/0214wireless2.html?fsrc=rss-wireless> (15 May 2010).
 8. For an eye opening article titled *Corporate Laptop Users put Businesses at Risk*, visit: <http://www.pcw.co.uk/computing/news/2071216/corporate-laptop-users-put-businesses-risk> (15 May 2010).
 9. For radio frequency identification (RFID), visit: <http://www.rfidjournal.com/faq> (15 May 2010).
 10. To read about PCMCIA cards, visit: http://support.3com.com/infodeli/inotes/techtran/4bb_a_5ea.htm (15 May 2010).
 11. Jackson, W. (2005) *GCN Staff Survey: Digital Gadgets take a Back Seat – and Stay there*, available at: <http://gcn.com/articles/2005/01/24/survey-digital-gadgets-take-a-back-seatand-stay-there.aspx> (15 May 2010).
 12. Middleton, J. (2001) Lost Mobile Devices drive Security Fears, Web article from the VNU Network VNU Business Publications, available at: <http://www.vnunet.com/articles/print/2115935> (15 May 2010).
 13. For further technical details of the AES algorithm, visit Rijndael home page at: <http://csrc.nist.gov/archive/aes/index.html> (15 May 2010).
 14. Shriraghavan, S., Sundaragopalan, S., Yang, F., and Jun, J. (2003) *Security in Mobile Computing – Focus on Wireless Security*, November 25, available at: http://www.cc.gatech.edu/classes/AY2004/cs4235a_fall/presentations/NetSecPres.pdf (15 May 2010).
 15. To learn about the RIM November 2006 report, visit: <http://wwwcomputing.co.uk/itweek/news/2169730/55-mobile-phones-left-london> (15 May 2010). http://www.theregister.co.uk/2001/08/31/62_000_mobiles_lost/ (15 May 2010).
 16. Strang, T. (2003) *Trends in Mobile Computing – From Mobile Phone to Context-Aware Service Platform*, German Aerospace Center (DLR), Oberpfaffenhofen, Germany, available at http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt38/Bln_Release.pdf (15 May 2010).
 17. For Windows advice on protecting sensitive information residing on mobile devices, *Windows Mobile-based Devices and Security: Protecting Sensitive Business Information*, available at: http://download.microsoft.com/download/4/7/c/47c9d8ec-94d4-472b-887d-4a9ccf194160/6.%20WM_Security_Final_print.pdf#search='RAS%20Server%20Security%20for%20Mobile%20Devices' (15 May 2010).
 18. To know scams that target you or your small business, visit: <http://www.scamwatch.gov.au/content/index.phtml/itemId/693900> (20 February 2010).
 19. To learn about mobile device security, visit: <http://www.securelist.com/en/analysis?pubid=170773606> (15 May 2010).
 20. To know about PCI-DSS Standard, visit: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (18 July 2010).
 21. For PCI compliance guide, visit: <http://www.picomplianceguide.org/> (18 July 2010).
- Books**
1. Mallick, M. (2003) *Mobile and Wireless Design Essentials*, Wiley DreamTech (India) Ltd., New Delhi, India.
 2. Nanavati, S., Thieme, M., and Nanavati, R. (2002) *Biometrics*, 1st edn, Wiley DreamTech (India) Ltd., New Delhi, India.
 3. Unhelkar, B. (2006) *Handbook of Research in Mobile Business: Technical, Methodological, and Social Perspectives*, IDEA Group, Hershey, PA, USA.

- 4.** Siegemund, F. and Flörkemeier, C. (2003) *Interaction in Pervasive Computing Settings using Bluetooth-enabled Active Tags and Passive RFID Technology together with Mobile Phones*, Institute for Pervasive Computing, Department of Computer Science, ETH Zurich, Switzerland.

Articles and Research Papers

- 1.** Godbole, N. (2003) *Mobile Computing: Security Issues in Hand-Held Devices*, Paper presented at NASONES 2003 National Seminar on Management and Business, 13–16 February 2006, Sydney, Australia. The paper is available in the following link: http://www.au-kbc.org/bpmain1/Security/EMO_SecurityWhitepaper.pdf#search='RAS%20Server%20Security%20for%20Mobile%20Devices' for Ericsson Mobile Organizer (EMO) Security Whitepaper (15 May 2010).
- 2.** Sadlier, G. (October 2003), Mobile Computing Security, INS White Paper.
- 3.** Godbole, N. and Unhelkar, B. (2006) *Security Issues in Mobile Computing*, Proceedings of the 2nd International Conference on Information Management and Business, February 13–16, 2006, Sydney, Australia.

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, D, E, L. These are provided in the companion CD.

4 Tools and Methods Used in Cybercrime

Learning Objectives

After reading this chapter, you will be able to:

- Understand about proxy servers and anonymizers.
- Learn about password cracking.
- Learn what keyloggers and Spywares do.
- Get an overview of virus and worms.
- Learn about Trojan Horses and backdoors.
- Understand what steganography is.
- Learn about DoS and DDoS attacks.
- Learn about SQL injection.
- Understand buffer overflow.
- Get an overview of wireless network hacking.

4.1 Introduction

In Chapter 2, we have learnt about how criminals/attackers plan cyberoffenses against an individual and/or against an organization. In Chapter 3, we have learnt how mobile technology plays an important role to launch cyberattacks. With this background, in this chapter, we will focus upon different forms of attacks through which attackers target the computer systems. There are various tools and techniques (see Box 4.1) and complex methodologies used to launch attacks against the target. Although discussing all of them is virtually impossible in a single chapter, yet still, we have provided an insight toward these techniques to enable the reader to understand how the computer is an indispensable tool for almost all cybercrimes. As the Internet and computer networks are integral parts of information systems, attackers have in-depth knowledge about the technology and/or they gain thorough knowledge about it. (See Section 10.4.2, Chapter 10 in CD.)

Network attack incidents reveal that attackers are often very systematic in launching their attacks (see Section 7.13, Chapter 7). The basic stages of an attack are described here to understand how an attacker can compromise a network here:

1. **Initial uncovering:** We have explained this in Chapter 2. Two steps are involved here. In the first step called as *reconnaissance*, the attacker gathers information, as much as possible, about the target by legitimate means – searching the information about the target on the Internet by Googling social networking websites and people finder websites. The information can also be gathered by surfing the public websites/searching news articles/press releases if the target is an organization/institute. In the second step, the attacker uncovers as much information as possible on the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges. From prevention perspective, at this stage, it is really not possible to detect the attackers because they have done nothing illegal as yet and so their information requests are considered legitimate.

Box 4.1 Scareware, Malvertising, Clickjacking and Ransomware

1. **Scareware:** It comprises several classes of scam software with malicious payloads (explained in chapter 1), or of limited or no benefit, which are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat, generally directed at an unsuspecting user. Some forms of Spyware and Adware also use scareware tactics. Some websites display pop-up advertisement windows or banners with text such as: "Your computer may be infected with harmful Spyware programs. Immediate removal may be required. To scan, click 'Yes' below." These websites can go as far as saying that a user's job, career or marriage would be at risk. Webpages displaying such advertisements for such products are often considered as scareware. Serious scareware applications qualify as rogue software.
2. **Malvertising:** It is a malicious advertising – malware + advertising – an online criminal methodology that appears focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user-supplied content publishing services common to the social networking space. Cybercriminals attempt to distribute malware through advertising. Possible vectors of attack include Malicious Code hidden within an advertisement, embedded into a webpage or within software which is available for download.
3. **Clickjacking:** It is a malicious technique of tricking netizens into revealing confidential information and/or taking control of their system while clicking on seemingly innocuous webpages. Clickjacking takes the form of embedded code and/or script which is executed without netizen's knowledge. Cybercriminals take the advantage of vulnerability across a variety of browsers and platforms to launch this type of attack, for example clicking on a button that appears to perform another function. The term "clickjacking" was coined by Jeremiah Grossman and Robert Hansen in 2008. The exploit is also known as User-Interface (UI) redressing.
4. **Ransomware:** It is computer malware that holds a computer system, or the data it contains, hostage against its user by demanding a ransom for its restoration. It typically propagates as a conventional computer worm, entering a system through, for example, vulnerability in a network service or an E-Mail attachment. It may then
 - disable an essential system service or lock the display at system start-up and
 - encrypt some of the user's personal files.
 In both cases, the malware may extort by
 - prompting the user to enter a code obtainable only after wiring payment to the attacker or sending an SMS message and accruing a charge;
 - urging the user to buy a decryption or removal tool.

Sources: <http://en.wikipedia.org/wiki/Scareware> (10 January 10); <http://www.anti-malvertising.com/> (10 January 10); <http://en.wikipedia.org/wiki/Clickjacking> (10 February 10); [http://en.wikipedia.org/wiki/Ransomware_\(malware\)](http://en.wikipedia.org/wiki/Ransomware_(malware)) (10 January 10).

2. **Network probe:** At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool (see Table 2.2) is used to discover exactly which services are running on the target system. At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion.
3. **Crossing the line toward electronic crime (E-crime):** Now the attacker is toward committing what is technically a "computer crime." He/she does this by exploiting possible holes on the target system. The attacker usually goes through several stages of exploits to gain access to the system. Certain programming errors can be used by attackers to compromise a system and are quite common in practice (see Table 4.1 for list of websites commonly browsed by attackers to obtain the information on the vulnerabilities). Exploits usually include vulnerabilities in common gateway interface (CGI) scripts or well-known buffer-overflow holes, but the easiest way to gain an entry is by checking for default login accounts with easily guessable (or empty) passwords. Once the attackers are able to access a user account without many privileges, they will attempt further exploits to get an administrator or "root" access. Root access is a Unix term

Table 4.1 | Websites and tools used to find the common vulnerabilities

<i>Website</i>	<i>Brief Description</i>
http://www.us-cert.gov/	US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). US-CERT also provides a way for citizens, businesses and other institutions to communicate and coordinate directly with the US government about cybersecurity. US-CERT publishes information about a variety of vulnerabilities under “US-CERT Vulnerabilities Notes.”
http://cve.mitre.org/	Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures and free for public use. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
http://secunia.com/	It has thousands of vulnerability lists that are updated periodically. It has vulnerability database and provides in-depth analysis about virus, worm alerts and software vulnerability.
http://www.hackerstorm.com/	This website was created for open-source vulnerability database (OSVBD) tool. Since then it has grown in popularity and provides additional information about penetration testing. The site is updated with whole bunch of news and alerts about vulnerability research.
http://www.hackerwatch.org/	It is an online community where Internet users can report and share information to block and identify security threats and unwanted traffic.
http://www.zone-h.org/	It reports on recent web attacks and cybercrimes and lists them on the website. One can view numerous defaced webpages and details about them.
http://www.milworm.com/	It contains day-wise information about exploits.
http://www.osvdb.org/	OSVDB: This is an open-source vulnerability database providing a large quantity of technical information and resources about thousands of vulnerabilities.
http://www.metasploit.com/	Metasploit is an open-source computer security project that provides information about security vulnerabilities and aids in penetration testing. Its most well-known subproject is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. The Metasploit Project is also well-known for antiforensic and evasion tools, some of which are built into the Metasploit Framework.
http://www.w00w00.org/files/ LibExploit	LibExploit is a generic exploit creation library. It helps cybersecurity community when writing exploits to test vulnerability.
http://www.immunitysec.com/products-canvas.shtml	Canvas is a commercial vulnerability exploitation tool from Dave Aitel's ImmunitySec. It includes more than 150 exploits and also available are VisualSploit Plugin for drag and drop GUI exploit creation (optional).
http://www.coresecurity.com/content/ core-impact-overview	Core Impact is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks such as exploiting one system and then establishing an encrypted tunnel through that system to reach and exploit other systems.

and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems). “Root” is basically an administrator or super-user access and grants them the privileges to do anything on the system.

4. **Capturing the network:** At this stage, the attacker attempts to “own” the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack. The attacker will usually install a set of tools that replace existing files and services with Trojan files (*Trojan Horse* is further discussed in detail in this chapter) and services that have a backdoor password. There are a number of “hacking tools” which can clean up log files and remove any trace of an intrusion; most of the time, they are individual programs written by hackers. Such tools provide copies of system files that look and act like real thing, but in fact they provide the attacker a backdoor entry into the system and hide processes he/she might be running on that system and his/her user information. This allows the attacker to return to the system at will, which means that the attacker has “captured” the network. Once the attacker has gained access to one system, he/she will then repeat the process by using the system as a stepping stone to access other systems deeper within the network, as most networks have fewer defenses against attacks from internal sources.
5. **Grab the data:** Now that the attacker has “captured the network,” he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.
6. **Covering tracks:** This is the last step in any cyberattack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected. The attacker can remain undetected for long periods or use this phase either to start a fresh reconnaissance to a related target system or continued use of resources, removing evidence of hacking, avoiding legal action, etc. (See Table 4.2 to know tools used to cover tracks.)

During this entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself. How is it possible is described in the next section.

Table 4.2 | Tools used to cover tracks

Sr. No.	Website	Brief Description
1	http://www.ibt.ku.dk/jesper/ ELSave/	ELSave: It is a tool to save and/or clear an NT event log. ELSave is written by Jesper Lauritsen. The executable is available on the weblink, but source code is not available.
2	http://ntsecurity.nu/ toolbox/winzapper/	WinZapper: This tool enables to erase event records selectively from the security log in Windows NT 4.0 and Windows 2000. This program corrupts the event logs, therefore, they must be cleared completely.
3	http://www.evidence- eliminator.com/	Evidence eliminator: It is simple and one of the top-quality professional PC cleaning program that is capable of defeating all known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis becomes impossible.
4	http://www.traceless.com/ computer-forensics/	Traceless: It is a privacy cleaner for Internet explorer (IE) that can delete common Internet tracks, including history, cache, typed URLs, cookies, etc.

(Continued)

Table 4.2 | (Continued)

<i>Sr. No.</i>	<i>Website</i>	<i>Brief Description</i>
5	http://www.acesoft.net/	<p>Tracks Eraser Pro: It deletes following history data:</p> <ul style="list-style-type: none"> • Delete address bar history of IE, Netscape, AOL, Opera. • Delete cookies of IE, Netscape, AOL, Opera. • Delete Internet cache (temporary Internet files). • Delete Internet history files. • Delete Internet search history. • Delete history of autocomplete. • Delete IE plugins (selectable). • Delete index.dat file. • Delete history of start menu run box. • Delete history of start menu search box. • Delete windows temp files. • Delete history of open/save dialog box. • Empty recycle bin.

4.2 Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connections with other computers on that network.

The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy. This enables an attacker to surf on the Web anonymously and/or hide the attack. A client connects to the proxy server and requests some services (such as a file, webpage, connection or other resource) available from a different server. The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client. Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for security reasons).
2. Speed up access to a resource (through “caching”). It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address (visit <http://www.multiproxy.org/multiproxy.htm> for more information).

One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time. In fact there are special servers available known as *cache servers*. A proxy can also do logging.

Listed are few websites where free proxy servers can be found:

1. <http://www.proxy4free.com>
2. <http://www.publicproxyservers.com>

3. <http://www.proxz.com>
4. <http://www.anonymitychecker.com>
5. <http://www.surf24h.com>
6. <http://www.hidemyass.com>

An *anonymizer* or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.^[1] Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client. In 1997 the first anonymizer software tool was created by Lance Cottrell, developed by Anonymizer.com. The anonymizer hides/removes all the identifying information from a user's computer while the user surfs on the Internet, which ensures the privacy of the user. (See Section 9.7, Chapter 9.)

Listed are few websites where more information about anonymizers can be found:

1. <http://www.anonymizer.com>
2. <http://www.browzar.com>
3. <http://www.anonymize.net>
4. <http://www.anonymouse.ws>
5. <http://www.anonymousindex.com>

Box 4.2 Being Anonymous While Searching on Google!

Google Cookie

Google was the first search engine to use a cookie.^[2] Google set the standard and nowadays cookies are commonplace among search engines. This cookie places a unique ID number on your hard disk. Anytime you visit Google, user gets a Google cookie if a user doesn't already have one. If a user has one then it will read and record the unique ID number. Google can build a detailed list of your search terms over many years. (Google's cookies are set to expire by the year 2038, unless a user deletes before its expiry.)

Cookie

Cookie (also known as HTTP cookie/browser cookie) is a small text file that contains a string of alphanumeric characters and is used for storing netizen's website preferences/authentication while visiting the same webpage again and again or also acts as identifier for server-based session – such browser mechanism of setting and reading cookies invites attackers to use these cookies as "Spyware." There are two types of cookies:

1. Persistent cookie and
2. session cookie.

Persistent cookie is stored by the web browser into the cookie folder on the PC's hard disk. It remains under the cookie folder, which is maintained by the web browser. Session cookie is a temporary cookie and does not reside on the PC once the browser is closed (see Boxes 9.2, 9.3 and 9.4, Chapter 9).

DoubleClick

It is a subsidiary of Google and provides Internet ad-serving services and paid search products listing (DART Search^[3]) and utilize the cookies, which are called DART cookie. Internet Advertising Network was started by Kevin O'Connor and Dwight Merriman in 1995. IAN and the DoubleClick division of Poppe-Tyson were merged into a new corporation named DoubleClick in 1996. DoubleClick was first in the online media representative business, that is, representing websites to sell advertising space to marketers. In 1997 it began offering the online ad serving and management technology they had

Box 4.2 Being Anonymous . . . (Continued)

developed to other publishers as the DART services. The DART cookie is a persistent cookie, which consists of the name of the domain that has set the cookie, the lifetime of the cookie and a "value." DoubleClick's DART mechanism generates a unique series of characters for the "value" portion of the cookie. These DoubleClick DART cookies help marketers learn how well their Internet advertising campaigns or paid search listings perform. Many marketers and Internet websites use DoubleClick's DART technology to deliver and serve their advertisements or manage their paid search listings. DoubleClick's DART products set or recognize a unique, persistent cookie when an ad is displayed or a paid listing is selected. The information that the DART cookie helps to give marketers includes the number of unique users their advertisements displayed to, how many users clicked on their Internet ads or paid listings and which ads or paid listings they clicked on.

G-Zapper

G-Zapper^[4] utility helps to stay anonymous while searching Google. Google stores a unique identifier in a cookie on the computer (i.e., on the hard disk) which allows to track keywords that are searched for. This information is used to compile reports, track user habits and test features. In the future, it would be possible that this information is sold and/or shared with others.

G-Zapper helps to protect users' ID and search history. G-Zapper reads the Google cookie installed on users' PC, displays the date it was installed, determines how long user searches have been tracked and displays Google searches. G-Zapper allows user to automatically delete or entirely block the Google search cookie from future installation.

This utility can be downloaded from <http://www.dummysoftware.com/gzapper.html>

4.3 Phishing

While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately. Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail. This message and other such messages are examples of Phishing – in addition to stealing personal and financial data – and can infect systems with viruses and also a method of online ID theft in various cases. Most people associate Phishing with E-Mail messages that spoof or mimic banks, credit card companies or other business such as Amazon and eBay. These messages look authentic and attempt to get users to reveal their personal information.



It is believed that *Phishing* is an alternative spelling of "fishing," as in "to fish for information." The first documented use of the word "Phishing" was in 1996.

4.3.1 How Phishing Works?

Phishers work in the following ways^[5]:

- Planning:** Criminals, usually called as phishers, decide the target (i.e., specific business/business house/an individual) and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques as spammers.
- Setup:** Once phishers know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves E-Mail addresses and a webpage.

3. **Attack:** This is the step people are most familiar with – the phisher sends a phony message that appears to be from a reputable source.
4. **Collection:** Phishers record the information of victims entering into webpages or pop-up windows.
5. **Identity theft and fraud:** Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Phishing started off as being part of popular hacking culture. Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level. We have explained Phishing and Identity Theft in detail in Chapter 5.

4.4 Password Cracking

Password is like a key to get an entry into computerized systems like a lock. Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.^[6] Usually, an attacker follows a common approach – repeatedly making guesses for the password. The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:

1. Find a valid user account such as an Administrator or Guest;
2. create a list of possible passwords;
3. rank the passwords from high to low probability;
4. key-in each password;
5. try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information (explained in Chapter 5). Examples of guessable passwords include:

1. Blank (none);
2. the words like "password," "passcode" and "admin";
3. series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertuyuiop;
4. user's name or login name;
5. name of user's friend/relative/pet;
6. user's birthplace or date of birth, or a relative's or a friend's;
7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;
9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list. This is still considered manual cracking, is time-consuming and not usually effective.

Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource. To ensure confidentiality of passwords, the

password verification data is usually not stored in a clear text format. For example, one-way function (which may be either an encryption function or a cryptographic hash) is applied to the password, possibly in combination with other data, and the resulting value is stored. When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with the stored value. If they match, user gains the access; this process is called *authentication*.

Even though these functions create hashed passwords, which may be cryptographically secure, an attacker attempts to get possession of the hashed password, which will help to provide a quick way to test guesses for the password by applying the one-way function to each guess and comparing the result to the verification data. The most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools (see Table 4.3) to get the plain text password.

Table 4.3 | Password cracking tools

Website	Brief Description
www.defaultpassword.com	Default password(s): Network devices such as switches, hubs and routers are equipped with “default passwords” and usually these passwords are not changed after commissioning these devices into the network (i.e., into LAN). The intruders can gain the access using these default passwords by visiting the said website.
http://www.oxid.it/cain.html	Cain & Abel: This password recovery tool is typically used for Microsoft Operating Systems (OSs). It allows to crack the passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force attacks, decoding scrambled passwords and recovering wireless network keys.
http://www.openwall.com/john	John the Ripper: This is a free and open-source software – fast password cracker, compatible with many OSs like different flavors of Unix, Windows, DOS, BeOS and OpenVMS. Its primary purpose is to detect weak Unix passwords.
http://freeworld.thc.org/thc-hydra	THC-Hydra: It is a very fast network logon cracker which supports many different services.
http://www.aircrack-ng.org	Aircrack-ng: It is a set of tools used for wireless networks. This tool is used for 802.11a/b/g wired equivalent privacy (WEP) and Wi-Fi Protected Access (WPA) cracking. It can recover a 40 through 512-bit WEP key once enough encrypted packets have been gathered. It can also attack WPA 1 or 2 networks using advanced cryptographic methods or by brute force.
http://www.l0phcrack.com	L0phCrack: It is used to crack Windows passwords from hashes which it can obtain from stand-alone Windows workstations, networked servers, primary domain controllers or Active Directory. It also has numerous methods of generating password guesses (dictionary, brute force, etc.).
http://airsnort.shmoo.com	AirSnort: It is a wireless LAN (WLAN) tool which recovers encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. It requires approximately 5–10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. It runs under Windows or Linux.

(Continued)

Table 4.3 | (Continued)

<i>Website</i>	<i>Brief Description</i>
http://www.solarwinds.com	SolarWinds: It is a plethora of network discovery/monitoring/attack tools and has created dozens of special-purpose tools targeted at systems administrators. Security-related tools include many network discovery scanners, a Simple Network Management Protocol (SNMP) brute force cracker, router password decryption and more.
http://www.fooftus.net/fizzgig/ pwdump	Pwdump: It is a Window password recovery tool. Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available.
http://project-rainbowcrack.com	RainbowCrack: It is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plain texts one by one, which can be time-consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called “rainbow tables.” It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.
http://www.hoobie.net/brutus	Brutus: It is one of the fastest, most flexible remote password crackers available for free. It is available for Windows 9x, NT and 2000. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP and more.

Password cracking attacks can be classified under three categories as follows:

1. Online attacks;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving are explained in Chapter 2).

4.4.1 Online Attacks

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as “bucket-brigade attack” or sometimes “Janus attack.” It is a form of active eavesdropping^[7] in which the attacker establishes a connection between a victim and the server to which a victim is connected. When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle). This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also be used to get the passwords for financial websites that would like to gain the access to banking websites.

4.4.2 Offline Attacks

Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used. Offline attacks usually require physical

Table 4.4 | Types of password cracking attacks

Type of Attack	Description	Example of a Password
Dictionary attack	Attempts to match all the words from the dictionary to get the password	Administrator
Hybrid attack	Substitutes numbers and symbols to get the password	Adm1n1strator
Brute force attack	Attempts all possible permutation-combinations of letters, numbers and special characters	Adm!n@09

access to the computer and copying the password file from the system onto removable media. Different types of offline password attacks are described in Table 4.4. Few tools listed in Table 4.2 also use these techniques to get the password in the clear text format.

4.4.3 Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords, such as words in the dictionary, proper names and words based on the username or common variations on these themes. Passwords that can be easily guessed by acquaintances of the netizens (such as date of birth, pet's name and spouses' name) are considered to be very weak. Here are some of the examples of "weak passwords":

1. **Susan:** Common personal name;
2. **aaaa:** repeated letters, can be guessed;
3. **rover:** common name for a pet, also a dictionary word;
4. **abc123:** can be easily guessed;
5. **admin:** can be easily guessed;
6. **1234:** can be easily guessed;
7. **QWERTY:** a sequence of adjacent letters on many keyboards;
8. **12/3/75:** date, possibly of personal importance;
9. **nbusr123:** probably a username, and if so, can be very easily guessed;
10. **p@\$\$/\\$/0rd:** simple letter substitutions are preprogrammed into password cracking tools;
11. **password:** used very often – trivially guessed;
12. **December12:** using the date of a forced password change is very common.

A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses it. The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker. A student's password might not be worth more than a few seconds of computer time, while a password controlling access to a large bank's electronic money transfer system might be worth many weeks of computer time for trying to crack it. Here are some examples of strong passwords:

1. **Convert_£100 to Euros!:** Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.
2. **382465304H:** It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly, for example, in schools and business.
3. **4pRte!ai@3:** It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.

4. MoOoOfIn245679: It is long with both alphabets and numerals.
5. t3wahSetyeT4: It is not a dictionary word; however, it has both alphabets and numerals.

Visit <http://www.microsoft.com/protect/fraud/passwords/checker.aspx> to check the strength of your password.^[8]

4.4.4 Random Passwords

We have explained in the previous section how most secure passwords are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters. The difficulty in remembering such a password increases the chance that the user will write down the password, which makes it more vulnerable to a different attack (in this case, the paper being lost or stolen and the password discovered). Whether this represents a net reduction in security depends on whether the primary threat to security is internal (e.g., social engineering) or external. A password can, at first sight, be random, but if you really examine it, it is just a pattern. One of these types of passwords is 26845. Although short, it is not easily guessed. However, the person who created the password is able to remember it because it is just the four direction keys on the square number board (found at the right of most keyboards) plus a five in the middle. If you practice it, it is just one swift motion of moving two fingers around the board (which is very easy to use). Forcing users to use system-created random passwords ensures that the password will have no connection with that user and should not be found in any dictionary. Several OSs have included such a feature. Almost all the OSs also include password aging; the users are required to choose new passwords regularly, usually after 30 or 45 days. Many users dislike these measures, particularly when they have not been taken through security awareness training. The imposition of strong random passwords may encourage the users to write down passwords, store them in personal digital assistants (PDAs) or cell phones and share them with others against memory failure, increasing the risk of disclosure.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names or phrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.
5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
6. User accounts should be frozen after five failed logon attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.
8. Successful logons should display the date and time of the last logon and logoff.
9. Logon IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Similarly, netizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber-attacks (explained in Section 3.8, Chapter 3).
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the weblinks displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks (we will explain Phishing attack in detail in Chapter 5).
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks (explained in detail in Chapter 3).
10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

4.5 Keyloggers and Spywares

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.^[9]

Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

4.5.1 Software Keyloggers

Software keyloggers are software programs (see Table 4.5) installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruses (will discuss more on this in subsequent sections of this chapter) without the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafes, library – we have already discussed this in Chapter 2) and can obtain the required information about the victim very easily. A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutible (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.^[10]

Table 4.5 | Software keyloggers

<i>Website</i>	<i>Brief Description</i>
http://www.soft-central.net	SC-KeyLog PRO: It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected logfile. SC-KeyLog PRO also captures Windows user logon passwords. The captured information is completely hidden from the user and allows to remotely install the monitoring system through an E-Mail attachment without the user recognizing the installation at all.
http://www.spytech-web.com	Spytech SpyAgent Stealth: It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.
http://www.relytec.com	All In One Keylogger: It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs. This keylogger allows secretly tracking of all activities from all computer users and automatically receiving logs to a desired E-Mail/FTP accounting. With this keylogger, one can read chat conversations, look at the E-Mails as well as watch the sites that have been surfed.
http://www.stealthkeylogger.org	Stealth Keylogger: It is a computer monitoring software that enables activity log report where the entire PC keyboard activities are registered either at specific time or hourly on daily basis. The entire log reports are generated either in text or HTML file format as defined by the user. The keylogger facilitates mailing of log report at the specified E-Mail address.
http://www.blazingtools.com	Perfect Keylogger: It has its advanced keyword detection and notification. User can create a list of “on alert” words or phrases and keylogger will continually monitor keyboard typing, URLs and webpages for these words or phrases – for example, “bomb,” “sex,” “visiting places around Mumbai” and “Windows vulnerabilities.” When a keyword is detected, perfect keylogger makes screenshot and sends E-Mail notification to the user.
http://kgb-spy-software.en.softonic.com	KGB Spy: It is a multifunctional keyboard tracking software, widely used by both regular users and IT security specialists. This program does not just record keystrokes but is also capable of recording language-specific characters. It records all typed data/all keyboard activity. It can be used to monitor children’s activity at home or to ensure employees do not use company’s computers inappropriately. Visit www.refog.com to find more on this product.
http://www.spy-guide.net/spybuddy-spy-software.htm	Spy Buddy: This, along with keylogger, has following features: <ul style="list-style-type: none"> • Internet conversation logging; • disk activity logging; • Window activity logging; • application activity logging; • clipboard activity logging; • AOL/Internet explorer history; • printed documents logging; • keylogger keystroke monitoring; • websites activity logging; • screenshot capturing; • WebWatch keyword alerting

(Continued)

Table 4.5 | (Continued)

<i>Website</i>	<i>Brief Description</i>
http://www.elite-keylogger.com	Elite Keylogger: It captures every keystroke typed, all passwords (including Windows logon passwords), chats, instant messages, E-Mails, websites visited, all program launched, usernames and time they worked on the computer, desktop activity, clipboard, etc.
http://www.cyberspysoftware.com	CyberSpy: It provides an array of features and easy-to-use graphical interface along with computer monitoring capabilities such as keep tabs on the employees and keeps track of what children are viewing on the Internet. CyberSpy can be used as complete PC monitoring solution for any home or office. CyberSpy records all websites visited, instant message conversations, passwords, E-Mails and all keystrokes pressed. It also has the ability to provide screenshots at set intervals.
http://www.mykeylogger.com	Powered Keylogger: Powered keylogger can be used for the following: <ul style="list-style-type: none"> • <i>Surveillance:</i> It is for anyone to control what happens on the computer when the computer's owner is away. • <i>Network administration:</i> It is for network administrators to control outgoing traffic and sites visited. • <i>Shared PC activity tracking:</i> It is to analyze the usage of shared PC. • <i>Parental control:</i> It helps parents to monitor their children's computer and Internet activity. • <i>Employee productivity monitoring:</i> It helps managers to check and increase productivity of their stuff or just to prevent the leak of important information.
http://www.x-pcsoft.com	XPC Spy: XPC Spy is one of the powerful keylogger spy software, runs stealthy under MS Windows and has the following features: <ul style="list-style-type: none"> • Records all keystrokes typed; • records all websites visited; • records all programs executed, folders explored, files opened or edited, documents printed, etc.; • records all windows opened; • records all clipboard text content; • records all system activities; • records webmails sent (database update online, more and more webmail servers are supported); • records all ICQ Messenger chat conversations; • records all MSN Messenger chat conversations; • records all AOL/AIM Messenger chat conversations; • records all Yahoo! Messenger chat conversations; • runs invisible in the background and is protected by password; • is built-in screenshot pictures viewer; • schedules monitor process, sets time to start or stop monitoring; • sends logs report via E-Mail.

4.5.2 Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs. Each keypress on the keyboard of the ATM gets registered by these keyloggers. These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Listed are few websites where more information about hardware keyloggers can be found:

1. <http://www.keyghost.com>
2. <http://www.keelog.com>
3. <http://www.keydevil.com>
4. <http://www.keykatcher.com>

4.5.3 Antikeylogger

Antikeylogger^[11] is a tool that can detect the keylogger installed on the computer system and also can remove the tool. Visit <http://www.anti-keyloggers.com> for more information.

Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

4.5.4 Spywares

Spyware is a type of malware (i.e., malicious software – see Box 4.3 to know about different types of malwares) that is installed on computers which collects information about users without their knowledge. The presence of Spyware is typically hidden from the user; it is secretly installed on the user's personal computer. Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.^[12]

It is clearly understood from the term *Spyware* that it secretly monitors the user. The features and functions of such Spywares are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users' computer system. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP). Various Spywares are available in the market and the one that are popular are listed in Table 4.6.

To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti-Spyware softwares (refer to Appendix B: List of Useful Software Utilities and Websites in CD) are available in the market. Installation of anti-Spyware software has become a common element nowadays from computer security practices perspective.

Box 4.3 Malwares

Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent (see Box 9.8, Chapter 9). The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code.^[13] Malware can be classified as follows:

1. **Viruses and worms:** These are known as *infectious malware*. They spread from one computer system to another with a particular behavior (will discuss more on this in Section 4.6).
2. **Trojan Horses:** A Trojan Horse,^[14] Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system (will discuss more on this in Section 4.7).
3. **Rootkits:** Rootkits^[15] is a software system that consists of one or more programs designed to obscure the fact that a system has been compromised. For further details refer to Section 7.12.1, Chapter 7.
4. **Backdoors:** Backdoor^[16] in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected.
5. **Spyware:** For further details see Section 4.5.
6. **Botnets:** For further details see Section 2.6 in Chapter 2.
7. **Keystroke loggers:** For further details see Section 4.5.

Table 4.6 | Spywares

Website	Brief Description
http://www.e-spy-software.com	007 Spy: It has following key features: <ul style="list-style-type: none"> • Capability of overriding “antspy” programs like “Ad-aware”; • record all websites URL visited in Internet; • powerful keylogger engine to capture all passwords; • view logs remotely from anywhere at anytime; • export log report in HTML format to view it in the browser; • automatically clean-up on outdated logs; • password protection.
http://www.spectorsoft.com	Spector Pro: It has following key features: <ul style="list-style-type: none"> • Captures and reviews all chats and instant messages; • captures E-Mails (read, sent and received); • captures websites visited; • captures activities performed on social networking sites such as MySpace and Facebook; • enables to block any particular website and/or chatting with anyone; • acts as a keylogger to capture every single keystroke (including usernames and passwords).
http://www.spectorsoft.com	eBlaster: Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording MySpace and Facebook activities and any other program activity.
http://www.remotespy.com	Remotespy: Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, it records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.

(Continued)

Table 4.6 | (Continued)

<i>Website</i>	<i>Brief Description</i>
http://www.topofbestsoft.com	Stealth Recorder Pro: It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features: <ul style="list-style-type: none"> • Real-time MP3 recording via microphone, CD, line-in and stereo mixer as MP3, WMA or WAV formatted files; • transferring via E-Mail or FTP, the recorded files to a user-defined E-Mail address or FTP automatically; • controlling from a remote location; • voice mail, records and sends the voice messages.
http://www.amplusnet.com	Stealth Website Logger: It records all accessed websites and a detailed report can be available on a specified E-Mail address. It has following key features: <ul style="list-style-type: none"> • Monitor visited websites; • reports sent to an E-Mail address; • daily log; • global log for a specified period; • log deletion after a specified period; • hotkey and password protection; • not visible in add/remove programs or task manager.
http://www.flexispy.com	Flexispy: It is a tool that can be installed on a cell/mobile phone. After installation, Flexispy secretly records cōversation that happens on the phone and sends this information to a specified E-Mail address.
http://www.wiretapro.com	Wiretap Professional: It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. This spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.
http://www.pcphonehome.com	PC PhoneHome: It is a software that tracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC PhoneHome has been installed, connected to the Internet, a stealth E-Mail is sent to a specified E-Mail address of the user's choice and to PC PhoneHome Product Company.
http://www.spyarsenal.com	SpyArsenal Print Monitor Pro: It has following features: <ul style="list-style-type: none"> • Keep track on a printer/plotter usage; • record every document printed; • find out who and when certain paper printed with your hardware.

4.6 Virus and Worms

Computer virus is a program that can “infect” legitimate programs by modifying them to include a possibly “evolved” copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random. Viruses can take some typical actions:

1. Display a message to prompt an action which may set off the virus;
2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

Figures 4.1–4.3 explain how viruses spread (a) through the Internet, (b) through a stand-alone computer system and (c) through local networks.

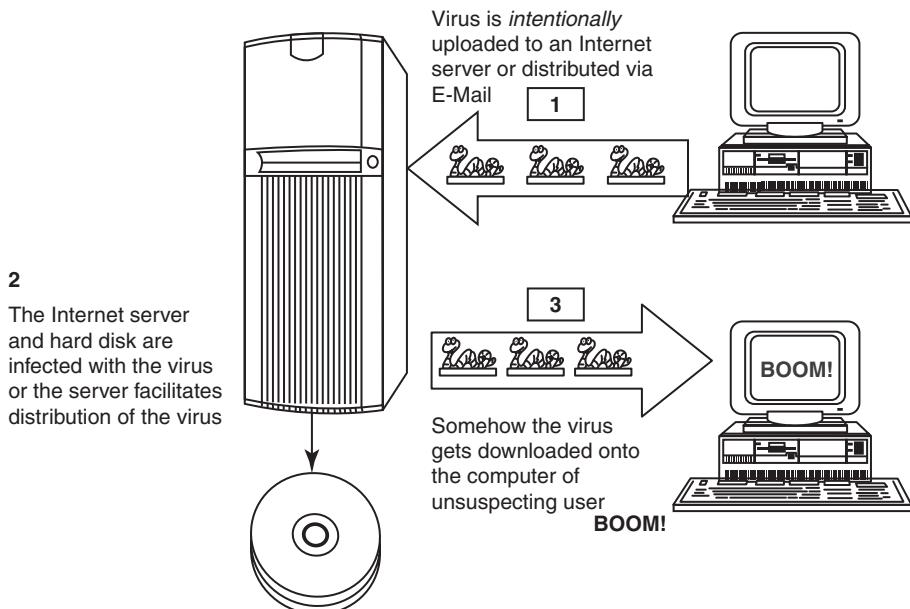


Figure 4.1 | Virus spreads through the Internet.

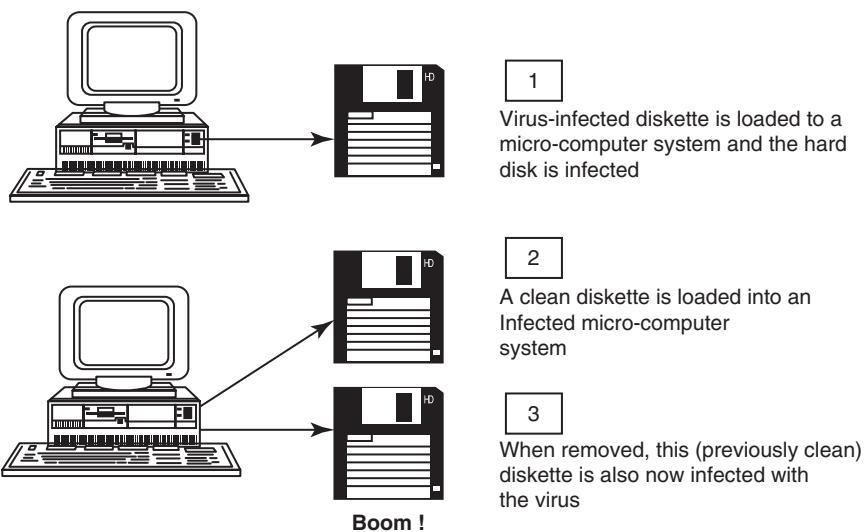


Figure 4.2 | Virus spreads through stand-alone system.

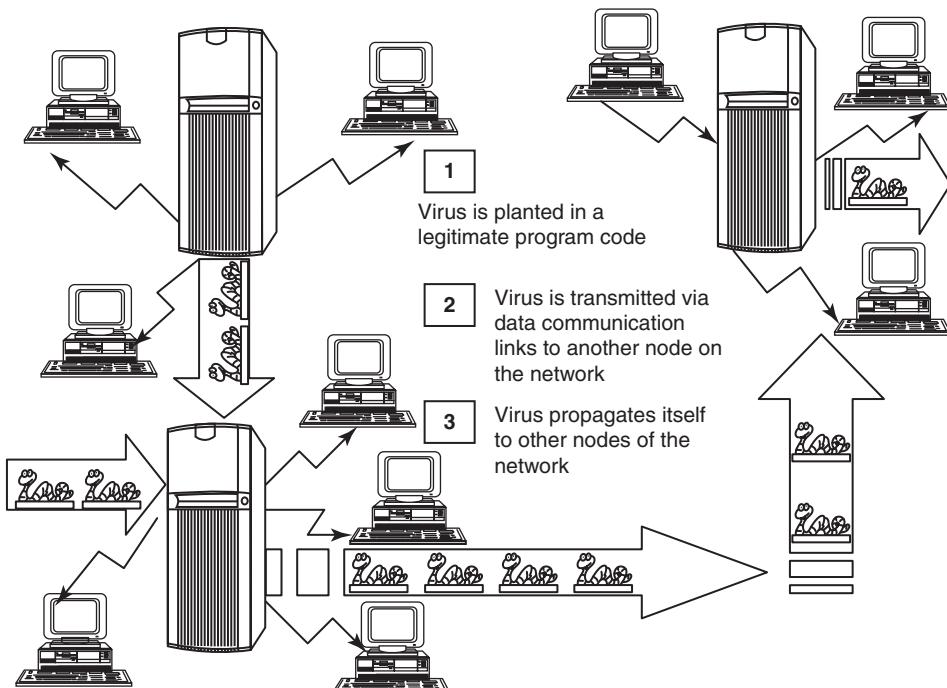


Figure 4.3 | Virus spreads through local networks.

Computer virus has the ability to copy itself and infect the system. The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability. A true virus can only spread from one system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives. Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.^[17]

As explained in earlier sections, the term *computer virus* is sometimes used as a *catch-all phrase* to include all types of malware, Adware and Spyware programs that do not have reproductive ability. Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, crimeware and other malicious and unwanted software as well as true viruses. Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different (see Table 4.7 to understand the difference between computer virus and worm). A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions. Worms and Trojans, such as viruses, may harm the system's data or performance. Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them. Some viruses do nothing beyond reproducing themselves.^[17]

Table 4.7 | Difference between computer virus and worm

Sr. No.	Facet	Virus	Worm
1	Different types	Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software program that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, <i>The Worm Programs</i> and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Source: See [18] in References section.

4.6.1 Types of Viruses

Computer viruses can be categorized^[19] based on attacks on various elements of the system and can put the system and personal data on the system in danger.

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., floppy diskettes and hard drives) and which is used to start the computer system. The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors. The first sector is called the BOOT and it carries the master boot record (MBR). MBR's function is to read and load OS, that is, it enables computer system to start through OS. Hence, if a virus attacks an MBR or infects the boot record of a disk, such floppy disk infects victim's hard drive when he/she reboots the system while the infected disk is in the drive. Once the victim's hard drive is infected all the floppy diskettes that are being used in the system will be infected. Boot sector viruses often spread to other systems when shared infected disks and pirated software(s) are used.
2. **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com, .exe, .ovl, .drv) is executed (i.e., opened – program is started). Once these program files get infected, the virus makes copies of itself and infects the other programs on the computer system.
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active. When the victim starts the computer system next time, it will infect the local drive and other programs on the victim's computer system.
4. **Stealth viruses:** It camouflages and/or masks itself and so detecting this type of virus is very difficult. It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system. It alters its file size and conceals itself in the computer memory to remain in the system undetected. The first computer virus, named as Brain, was a stealth virus. A good antivirus detects a stealth virus lurking on the victim's system by checking the areas the virus must have infected by leaving evidence in memory.
5. **Polymorphic viruses:** It acts like a "chameleon" that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program. *Polymorphic generators* are the routines (i.e., small programs) that can be linked with the existing viruses. These generators are not viruses but the purpose of these generators is to hide actual viruses under the cloak of polymorphism. The first all-purpose polymorphic generator was the mutation engine (MtE) published in 1991. Other known polymorphic generators are Dark Angel's Multiple Encryptor (DAME), Darwinian Genetic Mutation Engine (DGME), Dark Slayer Mutation Engine (DSME), MutaGen, Guns'n'Roses Polymorphic Engine (GPE) and Dark Slayer Confusion Engine (DSCE).
6. **Macroviruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROS (i.e., macrolanguages). These macros are programmed as a macroembedded in a document. Once a macrovirus gets onto a victim's computer then every document he/she produces will become infected. This type of virus is relatively new and may get slipped by the antivirus software if the user does not have the most recent version installed on his/her system.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls. Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work – such as enabling or disabling pop-ups, downloading files and sound – which invites the threats for the computer system being targeted by unwanted software(s) floating in cyberspace.

To know more on viruses see Box 4.4 and to know more on the world's worst virus attacks see Table 4.8. As Windows OS is the most used OS across the globe, the lists of viruses displayed in Table 4.8 are the attacks on Windows OS. The terms "Virus" and "Worm" are used interchangeably and hence readers may find that the viruses listed under Table 4.8 may be referred as worms on some websites and/or in some books.

Box 4.4 More about Viruses!

1. The early "hacking" sites that have allowed to download favorite virus are as follows:
 - www.2600.com
 - www.L0pht.com
2. The exhaustive list of viruses can be found at:
[http://en.wikipedia.org/wiki/List_of_computer_viruses_\(all\)](http://en.wikipedia.org/wiki/List_of_computer_viruses_(all))
3. The viruses can attack a system 365 days a year. However, on the designated payload dates, the viruses may do more than just infect the system. Virus calendar can be found at:
<http://home.mcafee.com/virusInfo/VirusCalendar.aspx>
4. **Computer virus hoax:** It is a message warning the recipient of a non-existent computer virus threat. The message is usually a chain E-Mail that tells the recipient to forward it to everyone they know. They often include announcements claimed to be from reputable organizations such as Microsoft, IBM or news sources such as CNN and include emotive language and encouragement to forward the message. These sources are quoted to add credibility to the hoax. The list of virus hoax can be found at:
http://en.wikipedia.org/wiki/Virus_hoax
5. **Unix and Linux OS are immune from computer viruses:** This is a myth that Unix/Linux systems are as susceptible to hostile software attacks as any other systems. However, such systems usually found to be well-protected compared with Microsoft Windows because fast updates are available to most Unix/Linux vulnerabilities. The list of virus/worms found on Unix/Linux systems can be found at:
http://en.wikipedia.org/wiki/Linux_malware

Table 4.8 | The world's worst virus attacks!!!

Sr. No.	Virus	Brief Description
1	Conficker	It is also known as Downup, Downadup and Kido. It targets Microsoft Windows OS and was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. The name Conficker is blended from a English term " <i>configure</i> " and the German word " <i>Ficker</i> ," which means "to have sex with" or "to mess with" in colloquial German.
2	INF/AutoRun	<i>AutoRun</i> and the companion feature <i>AutoPlay</i> are components of the Microsoft Windows OS that dictate what actions the system takes when a drive is mounted. This is the most common threat that infects a PC by creating an "autorun.inf" file. The file contains information about programs meant to run automatically when removable devices are connected to the computer. End-users must disable the AutoRun feature enabled by default in windows. AutoRun functionality is used in attack vector attacks.

(Continued)

Table 4.8 | (Continued)

<i>Sr. No.</i>	<i>Virus</i>	<i>Brief Description</i>
3	Win32 PSW. OnLineGames	It is a dangerous virus that replicates itself as other viruses and spreads from one computer system to another carrying a payload of destruction. It can infect several computers within few minutes. It is more concerned with gamers around the world, stealing confidential and other financial credentials as well as gaining access to the victim's account. This virus is also termed as Trojan.
4	Win32/Agent	This virus is also termed as Trojan. It copies itself into temporary locations and steals information from the infected system. It adds entries into the registry, creating several files at different places in the system folder, allowing it to run on every start-up, which enables to gather complete information about the infected system and then transferred to the intruder's system.
5	Win32/FlyStudio	It is known as Trojan with characteristics of backdoor. This virus does not replicate itself, but spreads only when the circumstances are beneficial. It is called as backdoors because the information stolen from a system is sent back to the intruder.
6	Win32/Pacex.Gen	This threat designates a wide range of malwares that makes use of an obfuscation layer to steal passwords and other information from the infected system.
7	Win32/Qhost	This virus copies itself to the System32 folder of the Windows directory giving control of the computer to the attacker. The attacker then modifies the Domain Name Server/System (DNS) settings redirecting the computer to other domains. This is done to compromise the infected machine from downloading any updates and redirect any attempts made to a website that downloads other malicious files on the victim's computer.
8	WMA/ TrojanDownloader. GetCodec	<p>This threat as the suffix .GetCodec modifies the audio files present on the system to ".wma" format and adds a URL header that points to the location of the new codec. In this manner, the host computer is forced to download the new codec and along with the new codec several other Malicious Codes are also downloaded.</p> <p>This means that the end-user will download the new codec believing that something new might happen, whereas the Malicious Code runs in the background causing harm to the host computer. At present, there is no way to verify the authenticity of the codec being downloaded as a new enhancement or a Trojan Horse; therefore, users must avoid unnecessary downloading of new codecs unless they are downloaded from a trusted website. Unnecessary downloading of codecs should also be avoided.</p>

Source: <http://www.brighthub.com/computing/smb-security/articles/44811.aspx>

A computer worm is a self-replicating malware computer program.^[20] It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.^[18] See Table 4.9 to know more on World's worst worm attacks.

Table 4.9 | The world's worst virus and worm attacks!!!

<i>Sr. No.</i>	<i>Worm</i>	<i>Brief Description</i>
1	Morris Worm	<p>It is also known as “Great Worm” or Internet Worm. It was written by a student, Robert Tappan Morris, at Cornell University and launched on 2 November 1988 from MIT. It was reported that around 6,000 major Unix machines were infected by the Morris worm and the total cost of the damage calculated was US\$ 10–100 millions.</p>
2	ILOVEYOU	<p>It is also known as VBS/Loveletter or Love Bug Worm. It successfully attacked tens of millions of Windows computers in 2000. The E-Mail was sent with the subject line as “ILOVEYOU” and an attachment “LOVE-LETTER-FOR-YOU.TXT.vbs.” The file extension “vbs” was hidden, hence the receiver downloads the attachment and opens it to see the contents.</p>
3	Nimda	<p>It is the most widespread computer worm and a file infector. It can affect Internet’s within 22 minutes. Nimda affected both user workstations (i.e., clients) running on Windows 95, 98, Me, NT, 2000 or XP and Servers running on Windows NT and 2000. It is “admin” when this worm’s name is spelled backward.</p>
4	Code Red	<p>This computer worm was observed on the Internet on 13 July 2001. It attacked computers running on Microsoft’s IIS web server.</p> <p>The Code Red worm was first discovered and researched by eEye Digital Security employees, Marc Maiffret and Ryan Permeh. They named the worm Code Red because they were drinking Pepsi’s “Mountain Dew Code Red” over the weekend. They analyzed it because of the phrase “Hacked by Chinese!” with which the worm defaced websites.</p> <p>On 4 August 2001 “Code Red II” appeared on the Internet and was found to be a variant of the original Code Red worm.</p>
5	Melissa	<p>It is also known as “Melissa,” “Simpsons,” “Kwyjibo” or “Kwejeebo.” It is a mass-mailing macro worm. Melissa was written by David L. Smith in Aberdeen Township, New Jersey, who named it after a lap dancer he met in Florida. The worm was in a file called “List.DOC” which had passwords that allow the access into 80 pornographic websites. This worm in the original form was sent through an E-Mail to many Internet users. Melissa spread on Microsoft Word 97, Word 2000 and also on Microsoft Excel 97, 2000 and 2003. It can mass-mail itself from E-Mail client Microsoft Outlook 97 or Outlook 98.</p>
6	MSBlast	<p>The Blaster Worm: It is also known as Lovsan or Lovesan, found during August 2003, which spread across the systems running on Microsoft Windows XP and Windows 2000. The worm also creates an entry under OS registry to launch the worm every time Windows starts. This worm contains two messages hidden in strings. The first, “I just want to say LOVE YOU SAN!!” and so the worm sometimes was called “Lovesan worm.” The second message, “Billy gates why do you make this possible? Stop making money and fix your software!!” This message was for Bill Gates, the co-founder of Microsoft and target of the worm.</p>
7	Sobig	<p>This worm, found during August 2003, infected millions of Internet-connected computers that were running on Microsoft Windows. It was written in Microsoft Visual C++ and compressed using a data compression tool, “tElock.” This Worm not only replicates by itself but also a Trojan Horse that it masquerades as something other than malware. It will appear as an E-Mail with one of the following subjects:</p> <ul style="list-style-type: none"> • Re: Approved • Re: Details

(Continued)

Table 4.9 | (Continued)

<i>Sr. No.</i>	<i>Worm</i>	<i>Brief Description</i>
		<ul style="list-style-type: none"> • Re: Re: My details • Re: Thank you! • Re: That movie • Re: Wicked screensaver • Re: Your application • Thank you! • Your details <p>It will contain the text as “See the attached file for details” or “Please see the attached file for details.” The E-Mail will also contain an attachment by one of the names mentioned below:</p> <ul style="list-style-type: none"> • application.pif • details.pif • document_9446.pif • document_all.pif • movie0045.pif • thank_you.pif • your_details.pif • your_document.pif • wicked_scr.scr
8	Storm Worm	<p>This worm, found on 17 January 2007, is also known as a backdoor Trojan Horse that affects the systems running on Microsoft OSs. The Storm worm infected thousands of computer systems in Europe and in the US on Friday, 19 January 2007, through an E-Mail with a subject line about a recent weather disaster, “230 dead as storm batters Europe.”</p> <p>The worm is also known as:</p> <ul style="list-style-type: none"> • Small.dam or Trojan-Downloader.Win32.Small.dam • CME-711 • W32/Nuwar@MM and Downloader-BAI • Troj/Dorf and Mal/Dorf • Trojan.DL.Tibs.Gen!Pac13 • TrojanDownloader-647 • Trojan.Peacomm • TROJ_SMALL.EDW • Win32/Nuwar • Win32/Nuwar.N@MM!CME-711 • W32/Zhelatin • Trojan.Peed, Trojan.Tibs
9	Michelangelo	<p>It is a worm discovered in April 1991 in New Zealand. This worm was designed primarily to infect the systems that were running on disk operating system (DOS) systems. Like other boot sector viruses, Michelangelo operated at the BIOS level and remained dormant until 6 March, the birthday of an artist “Michelangelo di Lodovico Buonarroti Simoni” – an Italian Renaissance painter, sculptor, architect and poet.</p>

(Continued)

Table 4.9 | (Continued)

Sr. No.	Worm	Brief Description
10	Jerusalem	This worm is also known as “BlackBox.” Jerusalem infected the files residing on DOS that was detected in Jerusalem, Israel, in October 1987. It has become memory resident (using 2 KB of memory). Once the system gets infected then it infects every executable file, except “COMMAND.COM.” “.COM” files grow by 1,813 bytes when infected by Jerusalem and are not reinfected. Similarly “.EXE” files grow from 1,808 to 1,823 bytes each time they get infected. Jerusalem reinfests “.EXE” files each time the file is loaded until their size is increased that is found to be “too large to load into memory.”

Almost every day new viruses/worms are created and they become new threat to netizens. (See Box 4.4 to know more about viruses.) In summary, in spite of different platforms (i.e., OS and/or applications), a typical definition of computer virus/worms might have various aspects^[21] such as:

1. A virus attacks specific file types (or files).
2. A virus manipulates a program to execute tasks unintentionally.
3. An infected program produces more viruses.
4. An infected program may run without error for a long time.
5. Viruses can modify themselves and may possibly escape detection this way.

4.7 Trojan Horses and Backdoors

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk. A Trojan Horse may get widely redistributed as part of a computer virus.^[22] The term Trojan Horse comes from Greek mythology about the Trojan War (see Box 4.5).

Box 4.5 Trojan War

The Trojan Horse is a tale from the Trojan War, as told in Virgil's Latin epic poem *The Aeneid* Quintus of Smyrna. The events in this story from the Bronze Age took place after Homer's *Iliad* and before his *Odyssey*. It was the stratagem that allowed the Greeks finally to enter the city of Troy and end the conflict. In the best-known version, after a fruitless 10-year siege, the Greeks construct a huge wooden horse in an attempt to once and for all destroy Troy from the inside. According to Quintus, it was Odysseus who came up with the idea of building a great wooden horse in which 30 men could hide to be wheeled into the city without the Trojans knowing. The Greeks build a huge, magnificent wooden horse in 3 days under the leadership of Epeios. Odysseus' plan also calls for one man to remain outside of the horse. This man will act as though the Greeks abandoned him, leaving the horse as a gift for the Trojans. The Greeks chose their soldier Sinon to play this role, as he is the only volunteer. Virgil describes the actual encounter between Sinon and the Trojans; Sinon successfully convinces the Trojans that he has been left behind and the Greeks are gone, and the horse is wheeled inside the city walls as a victory trophy. That night, the Greek soldiers hidden inside the horse emerged and opened the city gates for the rest of the Greek army. They raid and destroy the city of Troy, finally ending the Trojan War.

Source: http://en.wikipedia.org/wiki/Trojan_Horse (11 January 10).

Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet. It is also possible to inadvertently transfer malware through a USB flash drive or other portable media. It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines. (Users would not know that these could infect their network while bringing some music along with them to be downloaded.)

Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive. On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.

For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Visit http://en.wikipedia.org/wiki/List_of_trojan_horses to get the list of noteworthy Trojan Horses. Some typical examples of threats by Trojans^[23] are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.
6. They gather E-Mail addresses and use them for Spam.
7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

4.7.1 Backdoor

A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they detect or install themselves as part of an exploit. In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack^[24].

A backdoor works in background and hides from the user. It is very similar to a virus and, therefore, is quite difficult to detect and completely disable. A backdoor is one of the most dangerous parasites, as it allows a malicious person to perform any possible action on a compromised system. Most backdoors are autonomic malicious programs that must be somehow installed to a computer. Some parasites do not require installation, as their parts are already integrated into particular software running on a remote host. Programmers sometimes leave such backdoors in their software for diagnostics and troubleshooting purposes. Attackers often discover these undocumented features and use them to intrude into the system.

What a Backdoor Does?

Following are some functions of backdoor^[25]:

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.

2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission (see Section 7.13.7, Chapter 7).
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.
4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.
7. It distributes infected files to remote computers with certain security vulnerabilities and performs attacks against hacker-defined remote hosts.
8. It installs hidden FTP server that can be used by malicious persons for various illegal purposes.
9. It degrades Internet connection speed and overall system performance, decreases system security and causes software instability. Some parasites are badly programmed as they waste too many computer resources and conflict with installed applications.
10. It provides no uninstall feature, and hides processes, files and other objects to complicate its removal as much as possible.

Following are a few examples of backdoor Trojans:

1. **Back Orifice:** It is a well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS from a remote location. The name is a word play on Microsoft BackOffice Server software. Readers may visit <http://www.cultdeadcow.com/tools/bo.html> to know more about backdoor.
2. **Bifrost:** It is another backdoor Trojan that can infect Windows 95 through Vista. It uses the typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.
3. **SAP backdoors^[26]:** SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning. Backdoors can present into SAP User Master that supports an authentication mechanism when a user connects to access SAP and ABAP Program Modules which support SAP Business Objects.
4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests. Readers may visit <http://www.onapsis.com/research.html> to know more about this tool.

4.7.2 How to Protect from Trojan Horses and Backdoors

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. **Stay away from suspect websites/weblinks:** Avoid downloading free/pirated softwares that often get infected by Trojans, worms, viruses and other things. We have addressed "how to determine a legitimate website" in Chapter 5.
2. **Surf on the Web cautiously:** Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search that are used while surfing the information on the Web.

(See Box 4.6 to know more on P2P networks.) It may be experienced that, after downloading the file, it never works and here is a threat that – although the file has not worked, something must have happened to the system – the malicious software deploys its gizmos and the system is at serious health risk. Enabling Spam filter “ON” is a good practice but is not 100% foolproof, as spammers are constantly developing new ways to get through such filters.

3. **Install antivirus/Trojan remover software:** Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

Box 4.6 \ Peer-to-Peer (P2P) Networks

Peer-to-peer, commonly abbreviated as P2P, is any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances (such as servers or stable hosts). Peers are both suppliers and consumers of resources, in contrast to the traditional client–server model where only servers supply and clients consume.^[27] There are different levels of P2P networking^[28]:

1. **Hybrid P2P:** There is a central server that keeps information about the network. The peers are responsible for storing the information. If they want to contact another peer, they query the server for the address.
2. **Pure P2P:** There is absolutely no central server or router. Each peer acts as both client and server at the same time. This is also sometimes referred to as “serverless” P2P.
3. **Mixed P2P:** It is between “hybrid” and “pure” P2P networks. An example of such a network is Gnutella that has no central server but clusters its nodes around so-called “supernodes.”

Advantages of P2P Networks

1. It enables faster delivery of information from one computer to another by bypassing a central server.
2. It increases personal efficiency and personal empowerment. Users will no longer have to wait in queues to perform essential tasks, as all activities take place at the user’s discretion.
3. It represents significant cost savings over client/server models. As resources and computing power are distributed across the entire network, there is no need for expensive centralized servers; this will reduce the need for centralized management, storage and other related resources.
4. It offers easy scalability and all that is necessary for a network to grow is add more peers.
5. It increases a network’s fault tolerance. As no part of the system is essential to its operation, you can take down a few nodes and the network remains functional.
6. It leverages previously unused resources found on hundreds of millions of computers (and other services) that are connected to the “edges” of the Internet.
7. It frees up bandwidth on the Internet (or on a private network). In traditional client–server model, the server is the bottleneck and often cannot handle everything the client requests.
8. It requires no centralized management, oversight or control.
9. It offers increased privacy, as all data and messages are directly exchange between two computers.
10. It results in networks that are more flexible and adaptable compared with traditional client–server networks.

Besides all these advantages, there are still many reasons why P2P might not be the right model and is used only for specific set of activities.

Box 4.6 Peer-to-Peer . . . (Continued)

Drawbacks of P2P Networks

1. It propagates all sorts of undesirable items and activities including misinformation.
2. It increases network's, an individual system's, exposure to network attacks, viruses and other malicious damage.
3. It makes no guarantee that content/resources will always be available – any peer can go "dark" if he/she shuts down his/her computer.
4. It does not enforce content ownership (copyright).
5. It cannot enforce standards (either technological or ethical/moral/social).
6. It can be overwhelmed by increased traffic when it is unprepared (Napster uses many clogged university networks).
7. It is plagued by lack of standards, infrastructure and support. It is a kind of "Wild West" of the Internet.
8. Its transactions are difficult to translate into revenues streams and this lack of revenue generation could hinder its future development.

Ares, BitTorrent, Limewire and Kazaa are a few examples of popular P2P file-sharing programs. Readers may visit <http://www.bestsecuritytips.com/xfsection+article.articleid+49.htm> to know more on these popular P2P file-sharing programs.

Source: www.bus.ucf.edu/leigh/ism5937/linked/Ledesma_J.doc (17 May 2010).

4.8 Steganography

Steganography is a Greek word that means “sheltered writing.” It is a method that attempts to hide the existence of a message or communication. The word “steganography” comes from the two Greek words: steganos meaning “covered” and graphein meaning “to write” that means “concealed writing.” This idea of data hiding is not a novelty; it has been used for centuries all across the world under different regimes. The practice dates back to ancient Rome and Greece where the messages were etched into wooden tablets and then covered with wax or when messages were passed by shaving a messenger’s head and then tattooing a secret message on it, letting his hair grow back and then shaving it again after he arrived at the receiving party to reveal the message.

Given the sheer volume of data stored and transmitted electronically in the world today, it is no surprise that countless methods of protecting such data have evolved. One lesser known but rapidly growing method is steganography, the art and science of hiding information so that it does not even appear to exist! Steganography is always misunderstood with cryptography (see Box 4.7 to know difference between these two techniques). The different names for steganography are data hiding, information hiding (explained in Section 7.12.2, Chapter 7) and digital watermarking.

For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data. *Digital watermarking* is the process of possibly irreversibly embedding information into a digital signal. The signal may be, for example, audio, pictures or video. If the signal is copied then the information is also carried in the copy.^[29]

Box 4.7 Difference between Steganography and Cryptography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. It is said that terrorists use steganography techniques to hide their communication in images on the Internet; most popular images are used such as those of film actresses or other celebrities. In its basic form, steganography is simple. For example, say every fourth letter of a memo could hide a message. This simple technique has an added advantage over encryption that it does not arouse suspicion, that is, there is not much scope for getting started an investigation! Presence of an encryption could set off an investigation, but a message hidden in plain sight would get ignored (see Box 7.13, Chapter 7).

In October 2001, the New York Times published an article claiming that al-Qaeda had used steganographic techniques to encode messages into images, and then transported these via E-Mail and possibly via Usenet to prepare and execute the 11 September 2001 Terrorist Attack.^[30]

The term “cover” or “cover medium” is used to describe the original, innocent message, data, audio, still, video and so on. It is the medium that hides the secret message (see Fig. 4.4). It must have parts that can be altered or used without damaging or noticeably changing the cover media. If the cover media are digital, these alterable parts are called “redundant bits.” These bits or a subset can be replaced with the message that is intended to be hidden. Interestingly, steganography in digital media is very similar to “digital watermarking.” In other words, when steganography is used to place a hidden “trademark” in images, music and software, the result is a technique referred to as “watermarking” (see Table 4.10 to know more about steganography tools).

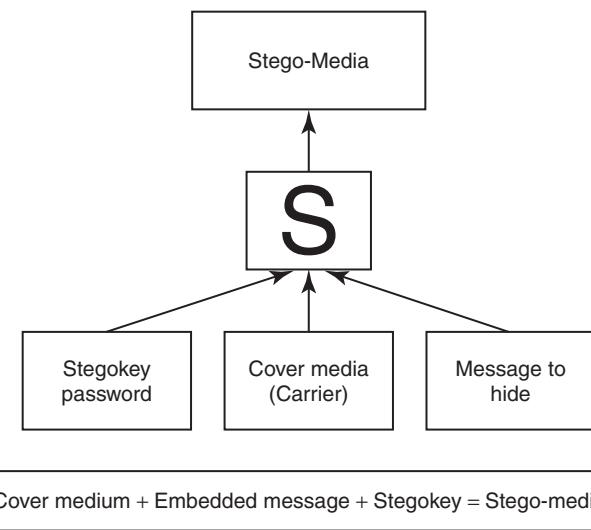


Figure 4.4 | How steganography works.

Source: <http://www.cosc.iup.edu/sezekiel/Seminar/steg.ppt#452,15,Steganography%20of%20today's%20talk> (11 May 10).

Table 4.10 | Steganography tools

<i>Website</i>	<i>Brief Description</i>
http://www.securityfocus.com	DiSi-Steganograph: It is a very small, DOS-based steganographic program that embeds data in PCX images.
http://www.brothersoft.com/invisible-folders-54597.html	Invisible Folders: It has the ability to make any file or folder invisible to anyone using your PC even on a network.
http://www.invisiblerecrets.com	Invisible Secrets: It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places such as picture or sound files or webpages. These types of files are a perfect disguise for sensitive information.
http://www.programurl.com/stealth-files.htm	Stealth Files: It hides any type of file in almost any other type of file. Using steganography technique, Stealth Files compresses, encrypts and then hides any type of file inside various types of files (including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP) and other types of video, image and executable files.
http://www.programurl.com/hermetic-stego.htm	Hermetic Stego: It is a steganography program that allows to encrypt and hide contents of any data file in another file so that the addition of the data to the container file will not noticeably change the appearance of that file. This program allows hiding a file of any size in one or more BMP image files with or without the use of a user-specified stego/encryption key so that (a) the presence of the hidden file is undetectable (even by forensic software using statistical methods) and (b) if a user-specified stego key is used then the hidden file can be extracted only by someone, using this software, who knows that stego key. DriveCrypt Plus (DCPP): It has following features: <ul style="list-style-type: none">• It allows secure hiding of an entire OS inside the free space of another OS.• Full-disk encryption (encrypts parts or 100% of your hard disk including the OS).• Preboot authentication (before the machine boots, a password is requested to decrypt the disk and start your machine).
http://www.securstar.com/products_drivecryptpp.php	MP3Stego: It hides information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.
http://compression.ru/video/stego_video/index_en.html	MSU StegoVideo: It allows hiding any file in a video sequence. Main features are as follows: <ul style="list-style-type: none">• Small video distortions after hiding information.• It is possible to extract information after video compression.• Information is protected with the password.



Steganography, Sudoku Puzzle and SMS: It is a revised version of information hiding (i.e., steganography) using Sudoku puzzle. This methodology was proposed by Chang *et al.* during 2008, which was inspired by Zhang and Wang's method and Sudoku solutions. Sudoku game has gained popularity recently and SMS is a popular medium of communication nowadays – messages are concealed into Sudoku puzzle, which are then communicated to intended recipient through SMS. As soon as recipient solves the puzzle, he/she can extract the data hidden into Sudoku puzzle image.

4.8.1 Steganalysis

Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography. The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it. Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files (see Table 4.11 for more details).

4.9 DoS and DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users.

4.9.1 DoS Attacks

In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent the Internet site or service from functioning efficiently or at all, temporarily or indefinitely. The attackers typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks and even root name servers (i.e., domain name

Table 4.11 | Steganalysis tools

<i>Website</i>	<i>Brief Description</i>
http://www.sarc-wv.com/products/stegalyzers.aspx	StegAlyzerAS: It is a digital forensic analysis tool designed to scan “suspect media” or “forensic images” of suspect media for known artifacts of steganography applications.
http://www.sarc-wv.com/stegalyzerss.aspx	StegAlyzerSS: It is a digital forensic analysis tool designed to scan “suspect media” or “forensic images” of suspect media for uniquely identifiable hexadecimal byte patterns, or known signatures, left inside files when particular steganography applications are used to embed hidden information within them.
http://www.spy-hunter.com/stegspy/download.htm	StegSpy: It is a program that is always in progress and the latest version includes identification of a “steganized” file. It detects steganography and the program used to hide the message. The latest version also identifies the location of the hidden content as well. StegSpy identifies programs such as Hiderman, JPHideandSeek, Masker, JpegX and Invisible Secrets.
http://www.outguess.org/detection.php	Stegdetect: It is an automated tool for detecting steganographic content in the images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images.
http://stegsecret.sourceforge.net	Stegsecret: It is a steganalysis open-source project that makes detection of hidden information possible in different digital media. It is a JAVA-based multiplatform steganalysis tool that allows the detection of hidden information by using the most known steganographic methods.
http://sourceforge.net/projects/vsl	Virtual Steganographic Laboratory (VSL): It is a graphical block diagramming tool that allows complex using, testing and adjusting of methods both for image steganography and steganalysis.

servers). Buffer overflow technique is employed to commit such kind of criminal attack known as *Spoofing*. The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system. A packet is a formatted unit of data carried by a packet mode computer network. The attacker spoofs the IP address and floods the network of the victim with repeated requests. As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request. This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.

The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:

1. Unusually slow network performance (opening files or accessing websites);
2. unavailability of a particular website;
3. inability to access any website;
4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

4.9.2 Classification of DoS Attacks

See Table 4.12 for classification of DoS attacks.

Table 4.12 | Classification of DoS attacks

<i>Sr. No.</i>	<i>DoS Attacks</i>	<i>Brief Description</i>
1	Bandwidth attacks	Loading any website takes certain time. Loading means complete webpage (i.e., with entire content of the webpage – text along with images) appearing on the screen and system is awaiting user's input. This "loading" consumes some amount of memory. Every site is given with a particular amount of bandwidth for its hosting, say for example, 50 GB. Now if more visitors consume all 50 GB bandwidth then the hosting of the site can ban this site. The attacker does the same – he/she opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth, thus, the site becomes out of service.
2	Logic attacks	These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.
3	Protocol attacks	Protocols here are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim's system to consume excess amounts of its resources.
4	Unintentional DoS attack	This is a scenario where a website ends up denied not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story. The result is that a significant proportion of the primary sites regular users', potentially hundreds of thousands of people, click that link within a few hours and have the same effect on the target website as a DDoS attack.

4.9.3 Types or Levels of DoS Attacks

There are several types or levels of DoS attacks as follows:

1. **Flood attack:** This is the earliest form of DoS attack and is also known as *ping flood*. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the “ping” command, which result into more traffic than the victim can handle. This requires the attacker to have a faster network connection than the victim (i.e., access to greater bandwidth than the victim). It is very simple to launch, but to prevent it completely is the most difficult.
2. **Ping of death attack:** The ping of death attack sends oversized Internet Control Message Protocol (ICMP) packets, and it is one of the core protocols of the IP Suite. It is mainly used by networked computers’ OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim. The maximum packet size allowed is of 65,536 octets. Some systems, upon receiving the oversized packet, will crash, freeze or reboot, resulting in DoS (e.g., the ping of death attack relied on a bug in the Berkeley TCP/IP stack, which also existed on most systems that copied the Berkeley network code).
3. **SYN attack:** It is also termed as *TCP SYN Flooding*. In the Transmission Control Protocol (TCP), handshaking of network connections is done with SYN and ACK messages. An attacker initiates a TCP connection to the server with an SYN (using a legitimate or spoofed source address). The server replies with an SYN-ACK. The client then does not send back an ACK, causing the server (i.e., target system) to allocate memory for the pending connection and wait. This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system. Figure 4.5 explains how the DoS attack takes place.

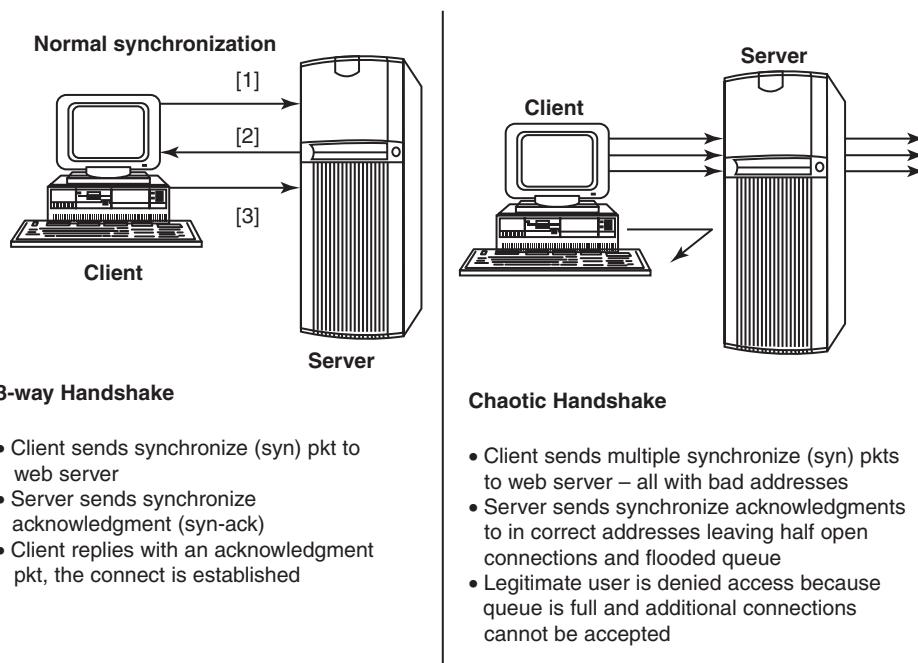


Figure 4.5 | Denial-of-service (DoS) attack.

4. **Teardrop attack:** The teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code. Windows 3.1x, Windows 95 and Windows NT OSs as well as versions of Linux (i.e., prior to versions 2.0.32 and 2.1.63) are vulnerable to this attack.^[31]
5. **Smurf attack:** It is a way of generating significant computer network traffic on a victim network. This is a type of DoS attack that floods a target system via spoofed broadcast ping messages. This attack consists of a host sending an ICMP echo request (ping) to a network broadcast address (e.g., network addresses with the host portion of the address having all 1s). Every host on the network receives the ICMP echo request and sends back an ICMP echo response inundating the initiator with network traffic. On a multi-access broadcast network, hundreds of machines might reply to each packet. This creates a magnified DoS attack of ping replies, flooding the primary victim. Internet relay chat (IRC) servers are the primary victim of smurf attacks on the Internet [(IRC is a form of real-time Internet text messaging (chat) or synchronous conferencing)].
6. **Nuke:** Nuke^[32] is an old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target. It is achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop. A specific example of a nuke attack that gained some prominence is the WinNuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a *Blue Screen of Death* (BSOD).

4.9.4 Tools Used to Launch DoS Attack

Various tools (see Table 4.13) use different types of traffic to flood a victim, but the objective behind the attack and the result is the same: A service on the system or the entire system (i.e., application/website/network) is unavailable to a user because it is kept busy trying to respond to an exorbitant number of requests. A DoS attack is usually an attack of last resort because it is considered to be an unsophisticated attack as the attacker does not gain access to any information but rather annoys the target and interrupts the service. (See Box 4.8 to know more about blended threats and Box 4.9 for PDoS attacks.)

Table 4.13 | Tools used to launch DoS attack

Sr. No.	Tool	Brief Description
1	Jolt2	A major vulnerability has been discovered in Windows' networking code. The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines – the attack causes the target machine to consume 100% of the CPU time on processing of illegal packets.
2	Nemesy	This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.
3	Targa	It is a program that can be used to run eight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successful.
4	Crazy Pinger	This tool could send large packets of ICMP to a remote target network.
5	SomeTrouble	It is a remote flooder and bomber. It is developed in Delphi.

Box 4.8 Blended Threat

Blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan Horses and Malicious Code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, transmit and thereafter spread an attack. Characteristics of blended threats are that

1. They cause harm to the infected system or network.
2. They propagate using multiple methods as attack may come from multiple points.
3. They also exploit vulnerabilities.

To be considered a blended threat, the attack would normally serve to transport multiple attacks in one payload. For example, it would not only just launch a DoS attack but it would also, for example, install a backdoor and maybe even damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. Therefore, while a worm may travel and spread through E-Mail, a single blended threat could use multiple routes including E-Mail, IRC and file-sharing networks.

Finally, rather than a specific attack on predetermined ".exe" files, a blended threat could do multiple malicious acts, such as modify your ".exe" files, HTML files and registry keys at the same time – basically it can cause damage to several areas of your network at one time.

Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats require no human intervention to propagate.

Source: <http://www.webopedia.com/didyouknow/internet/2004/virus.asp> (11 January 2010).

Box 4.9 Permanent Denial-of-Service (PDoS) Attack

A PDoS attack damages a system so badly that it requires replacement or reinstallation of hardware. Unlike DDoS attack – which is used to sabotage a service or website or as a cover for malware delivery – PDoS is a pure hardware sabotage. It exploits security flaws that allow remote administration on the management interfaces of the victim's hardware, such as routers, printers or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt or defective firmware image – a process which when done legitimately is known as *flashing*. Owing to these features, and the potential and high probability of security exploits on network-enabled-embedded devices (NEEDs), this technique has come to the attention of numerous hacker communities. PhlashDance is a tool created by Rich Smith (an employee of Hewlett-Packard's Systems Security Lab) who detected and demonstrated PDoS vulnerabilities at the 2008 EUsecWest Applied Security Conference in London.

Source: http://en.wikipedia.org/wiki/Denial-of-service_attack (11 May 2010).

4.9.5 DDoS Attacks

In a DDoS attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the DoS attack.

A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems (as explained in Chapter 1) are called "secondary victims" and the main target is called "primary victim."

Table 4.14 | Tools used to launch DDoS attack

Sr. No.	Tool	Brief Description
1	Trinoo	It is a set of computer programs to conduct a DDoS attack. It is believed that Trinoo networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploit.
2	Tribe Flood Network (TFN)	It is a set of computer programs to conduct various DDoS attacks such as ICMP flood, SYN flood, UDP flood and Smurf attack.
3	Stacheldraht	It is written by Random for Linux and Solaris systems, which acts as a DDoS agent. It combines features of Trinoo with TFN and adds encryption.
4	Shaft	This network looks conceptually similar to a Trinoo; it is a packet flooding attack and the client controls the size of the flooding packets and duration of the attack.
5	MStream	It uses spoofed TCP packets with the ACK flag set to attack the target. Communication is not encrypted and is performed through TCP and UDP packets. Access to the handler is password protected. This program has a feature not found in other DDoS tools. It informs all connected users of access, successful or not, to the handler(s) by competing parties.

Malware can carry DDoS attack mechanisms – one of the better-known examples of this is MyDoom. Typically, DoS mechanism triggered on a specific date and time. This type of DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack. A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent. Nowadays, Botnet (as explained in Chapter 2) is the popular medium to launch DoS/DDoS attacks. Attackers can also break into systems using automated tools (see Table 4.14) that exploit flaws in programs that listen for connections from remote hosts.

4.9.6 How to Protect from DoS/DDoS Attacks

Computer Emergency Response Team Coordination Center (CERT/CC) offers many preventive measures from being a victim of DoS attack.^[33]

1. Implement router filters. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
4. Enable quota systems on your OS if they are available.
5. Observe your system's performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, central processing unit (CPU) usage or network traffic.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files (see Table 4.15).
8. Invest in and maintain “hot spares” – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

Table 4.15 | Tools for detecting DoS/DDoS attacks

Sr. No.	Tool	Brief Description
1	Zombie Zapper	It is a free, open-source tool that can tell a zombie system flooding packets to stop flooding. It works against Trinoo, TFN and Stacheldraht. It assumes various defaults are still in place used by these attack tools, however, it allows you to put the zombies to sleep.
2	Remote Intrusion Detector (RID)	It is a tool developed in "C" computer language, which is a highly configurable packet snooper and generator. It works by sending out packets defined in the config.txt file, then listening for appropriate replies. It detects the presence of Trinoo, TFN or Stacheldraht clients.
3	Security Auditor's Research Assistant (SARA)	It gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws such as incorrectly set up or configured network services, well-known bugs in the system or network utilities system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database and weak policy decisions.
4	Find_DDoS	It is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.
5	DDoSPing	It is a remote network scanner for the most common DDoS programs. It can detect Trinoo, Stacheldraht and Tribe Flood Network programs running with their default settings.



Computer Emergency Response Team Coordination Center (CERT/CC) was started in December 1988 by the Defense Advanced Research Projects Agency, which was part of the US Department of Defense, after the Morris Worm disabled about 10% of all computers connected to the Internet. It is located at the Software Engineering Institute, a federally funded research center operated by Carnegie Mellon University. It studies Internet security vulnerabilities and provides services to websites that have been attacked. It also publishes security alerts.

Source: <http://www.webopedia.com/TERM/C/CERTCC.html> (31 May 2010).

4.10 SQL Injection

Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS). SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.^[34]

Attackers target the SQL servers – common database servers used by many organizations to store confidential data. The prime objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit card numbers, social security numbers or passwords. During an SQL injection attack, Malicious Code is inserted into a web form

field or the website's code to make a system execute a command shell or other arbitrary commands. Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field. For example, an arbitrary command from an attacker might open a command prompt or display a table from the database. This makes an SQL server a high-value target and therefore a system seems to be very attractive to attackers.

The attacker determines whether a database and the tables residing into it are vulnerable, before launching an attack. Many webpages take parameters from web user and make SQL query to the database. For example, when a user logs in with username and password, an SQL query is sent to the database to check if a user has valid name and password. With SQL injection, it is possible for an attacker to send crafted username and/or password field that will change the SQL query.

4.10.1 Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.
2. To check the source code of any website, right click on the webpage and click on "view source" (if you are using IE – Internet Explorer) – source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code. Everything between the <FORM> and </FORM> have potential parameters that might be useful to find the vulnerabilities.


```
<FORM action=Search/search.asp method=post>
<input type=hidden name=A value=C>
</FORM>
```
3. The attacker inputs a *single quote* under the text box provided on the webpage to accept the user-name and password. This checks whether the user-input variable is sanitized or interpreted literally by the server. If the response is an error message such as *use "a" = "a"* (or something similar) then the website is found to be susceptible to an SQL injection attack.
4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

Here are few examples of variable field text the attacker uses on a webpage to test for SQL vulnerabilities:

1. *Blah' or 1=1--*
2. *Login:blah' or 1=1--*
3. *Password::blah' or 1=1--*
4. *http://search/index.asp?id=blah' or 1=1--*

Similar SQL commands may allow bypassing of a login and may return many rows in a table or even an entire database table because the SQL server is interpreting the terms literally. The double dashes near the end of the command tell SQL to ignore the rest of the command as a comment.

Blind SQL Injection

Blind SQL injection^[34] is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be the one that displays data; however, it will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack can become time-intensive because a new statement must be crafted for each bit recovered. There are several tools that can automate these attacks once the location

of the vulnerability and the target information have been established. Readers may refer to Ref. #7, Additional Useful Web References, Further Reading to know about white paper.

In summary, using SQL injections, attackers can:

1. Obtain some basic information if the purpose of the attack is reconnaissance
 - To get a directory listing: Blah' ;exec master..xp_cmdshell "dir c:.*.* /s >c:\directory.txt";
 - To ping an IP address: Blah' ;exec master..xp_cmdshell "ping 192.168.1.1".
2. May gain access to the database by obtaining username and their password
 - To get a user listing: SELECT * FROM users WHERE name = "OR '1' = '1'."
3. Add new data to the database
 - Execute the INSERT command: This may enable selling politically incorrect items on an E-Commerce website.
4. Modify data currently in the database
 - Execute the UPDATE command: May be used to have an expensive item suddenly be deeply "discounted."



mySQLenum: It is a command line automatic blind SQL injection tool for web application that uses MySQL server as its back-end. The main objective of this tool is to provide an easy-to-use command line interface. Readers may visit <http://pentestit.com/2010/01/15/mysqlenum-automatic-blind-sql-injection-tool/> to know more on this tool.

See Table 4.16 to know some automated tools that are used either to find database vulnerabilities and/or to protect the database applications.

Table 4.16 | Tools used for SQL Server penetration

Sr. No.	Tool	Brief Description
1	http://www.appsecinc.com	AppDetectivePro: It is a network-based, discovery and vulnerability assessment scanner that discovers database applications within the infrastructure and assesses security strength. It locates, examines, reports and fixes security holes and misconfigurations as well as identify user rights and privilege levels based on its security methodology and extensive knowledge based on application-level vulnerabilities. Thus, organizations can harden their database applications.
2	http://www.appsecinc.com	DbProtect: It enables organizations with complex, heterogeneous environments to optimize database security, manage risk and bolster regulatory compliance. It integrates database asset management, vulnerability management, audit and threat management, policy management, and reporting and analytics for a complete enterprise solution.
3	http://www.iss.net	Database Scanner: It is an integrated part of Internet Security Systems' (ISS) Dynamic Threat Protection platform that assesses online business risks by identifying security exposures in the database applications. Database scanner offers security policy generation and reporting functionality, which instantly measures policy compliance and automates the process of securing critical online business data. Database scanner runs independently of the database and quickly generates detailed reports with all the information needed to correctly configure and secure databases.

(Continued)

Table 4.16 | (Continued)

<i>Sr. No.</i>	<i>Tool</i>	<i>Brief Description</i>
4	http://www.ca.com/us/ securityadvisor	SQLPoke: It is an NT-based tool that locates Microsoft SQL (MSSQL) servers and tries to connect with the default System Administrator (SA) account. A list of SQL commands are executed if the connection is successful.
5	http://www.ngssoftware. com/	NGSQLCrack: It can guard against weak passwords that make the network susceptible to attack. This is a password cracking utility for Microsoft SQL server 7 and 2000 and identifies user accounts with weak passwords so that they can be reset with stronger ones, thus, protecting the overall integrity of the system.
6	http://www.security- database.com/toolswatch	Microsoft SQL Server Fingerprint (MSSQLFP) Tool: This is a tool that performs fingerprinting version on Microsoft SQL Server 2000, 2005 and 2008, using well-known techniques based on several public tools that identifies the SQL version and also can be used to identify vulnerable versions of Microsoft SQL Server

4.10.2 How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. **Input validation**
 - Replace all single quotes (escape quotes) to two single quotes.
 - Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character sequences such as ; , --, select, insert and xp_ can be used to perform an SQL injection attack.
 - Numeric values should be checked while accepting a query string value. Function – IsNumeric() for Active Server Pages (ASP) should be used to check these numeric values.
 - Keep all text boxes and form fields as short as possible to limit the length of user input.
2. **Modify error reports:** SQL errors should not be displayed to outside users and to avoid this, the developer should handle or configure the error reports very carefully. These errors sometimes display full query pointing to the syntax error involved and the attacker can use it for further attacks.
3. **Other preventions**
 - The default system accounts for SQL server 2000 should never be used.
 - Isolate database server and web server. Both should reside on different machines.
 - Most often attackers may make use of several extended stored procedures such as xp_cmdshell and xp_grantlogin in SQL injection attacks. In case such extended stored procedures are not used or have unused triggers, stored procedures, user-defined functions, etc., then these should be moved to an isolated server.

These are the minimum countermeasures that can be implemented to prevent SQL injection attack. Technocrats may want to know more on this topic and can go through Refs. #8 and #9, Additional Useful Web References.



SQLBlock: SQLBlock is an open data base connectivity (ODBC) driver that acts as an SQL injection protection feature. It blocks the execution and sends an alert to administrator, in case of any client-application attempt to execute any disallowed SQL statements. It works as an ordinary ODBC data source and monitor every SQL statements being executed.

4.11 Buffer Overflow

Buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data. This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash) or a breach of system security.

Buffer overflows can be triggered by inputs that are designed to execute code or alter the way the program operates. They are, thus, the basis of many software vulnerabilities and can be maliciously exploited. Bounds checking can prevent buffer overflows.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type), which is within the boundaries of that array.^[35]

Buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. As buffers are created to contain a finite amount of data, the extra information – which has to go somewhere – can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

The knowledge of C, C++ or any other high-level computer language (i.e., assembly language) is essential to understand buffer overflow, as basic knowledge of process memory layout is very important. A buffer is a contiguous allocated chunk of memory such as an array or a pointer in C. In C and C++, there are no automatic bounds checking on the buffer – which means a user can write past a buffer. For example,

```
int main () {
    int buffer[10];
    buffer[20] = 10;
}
```

This C program is a valid program and every compiler can compile it without any errors. However, the program attempts to write beyond the allocated memory for the buffer, which might result in an unexpected behavior.

4.11.1 Types of Buffer Overflow

Stack-Based Buffer Overflow

Stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer. Here are the characteristics of stack-based programming:

1. “Stack” is a memory space in which automatic variables (and often function parameters) are allocated.
2. Function parameters are allocated on the stack (i.e., local variables that are declared on the stack – unless they are also declared as “static” or “register”) and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.

3. Once a function has completed its cycle, the reference to the variable in the stack is removed. (Therefore, if a function is called multiple times, its local variables and parameters are recreated and destroyed each time the function is called and exited.)

The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting:

1. A local variable that is near the buffer in memory on the stack to change the behavior of the program that may benefit the attacker.
2. The return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input-filled buffer.
3. A function pointer, or exception handler, which is subsequently executed.

The factors that contribute to overcome the exploits are

1. Null bytes in addresses;
2. variability in the location of shellcode;
3. differences between environments.



A shellcode is a small piece of code used as a payload in the exploitation of software vulnerability. It is called “shellcode” because it starts with command shell from which the attacker can control the compromised machine.

NOPs

NOP or NOOP (short form of no peration or no operation performed) is an assembly language instruction/command that effectively does nothing at all. The explicit purpose of this command is not to change the state of status flags or memory locations in the code. This means NOP enables the developer to force memory alignment to act as a place holder to be replaced by active instructions later on in program development.

NOP opcode can be used to form an NOP slide, which allows code to execute when the exact value of the instruction pointer is indeterminate (e.g., when a buffer overflow causes a function’s return address on the stack to be overwritten). It is the oldest and most widely used technique for successfully exploiting a stack buffer overflow. It helps to know/locate the exact address of the buffer by effectively increasing the size of the target stack buffer area. The attacker can increase the odds of findings the right memory address by padding his/her code with NOP operation. To do this, much larger sections of the stack are corrupted with the NOOP machine instruction. At the end of the attacker-supplied data, after the NOOP instructions, an instruction is placed to perform a relative jump to the top of the buffer where the shellcode is located. This collection of NOOP is referred to as the “NOP sled” because if the return address is overwritten with any address within the NOOP region of the buffer then it will “slide” down the NOOP until it is redirected to the actual Malicious Code by the jump at the end. This technique requires the attacker to guess where in the stack the NOP sled is compared with small shellcode.

Owing to the popularity of this technique, many vendors of intrusion prevention system will search for this pattern of NOOP machine instructions in an attempt to detect shellcode in use. It is important to note that an NOP sled does not necessarily contain only traditional NOOP machine instructions but also any instruction that does not corrupt the state of machine to a point where the shellcode will not run and can be used in place of the hardware-assisted NOOP. As a result, it has become common practice for exploit writers to compose the NOOP sled with randomly chosen instructions that will have no real effect on the shellcode execution.^[35]

Heap Buffer Overflow

Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. In either case, the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain. A routine is vulnerable to exploitation if it copies data to a buffer without first verifying that the source will fit into the destination. The characteristics of stack-based and heap-based programming are as follows:

1. “Heap” is a “free store” that is a memory space, where dynamic objects are allocated.
2. The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions; it is different from the memory space allocated for stack and code.
3. Dynamically created variables (i.e., declared variables) are created on the heap before the execution program is initialized to zeros and are stored in the memory until the life cycle of the object has completed.

Memory on the heap is dynamically allocated by the application at run-time and normally contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc metadata) and uses the resulting pointer exchange to overwrite a program function pointer.

4.11.2 How to Minimize Buffer Overflow

Although it is difficult to prevent all possible attacks, the following methods will definitely help to minimize such attacks:

1. **Assessment of secure code manually:** Buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold. Developers should be educated about minimizing the use of vulnerable functions available in C library, such as strcpy(), strcat(), sprintf() and vsprintf(), which operate on null-terminated strings and perform no bounds checking. The input validation after scanf() function that reads user input into a buffer is very essential.
2. **Disable stack execution:** Malicious Code causes input argument to the program, and it resides in the stack and not in the code segment. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation. Therefore, the simplest solution is to invalidate the stack to execute any instructions. However, the solution is not easy to implement. Although possible in Linux, some compilers [(including GNU Compliance Connection (GCC)] use trampoline functions to implement taking the address of a nested function that works on the system stack being executable. A trampoline is a small piece of code created at run-time when the address of a nested function is taken. It normally resides in the stack and in the stack frame of the containing function and thus requires the stack to be executable. However, a version of the Linux kernel that enforces the non-executable stack is freely available.
3. **Compiler tools:** Over the years, compilers have become more and more aggressive in optimizations and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as gets(), strcpy(), etc. Developers should be educated to restructure the programming code if such warnings are displayed.
4. **Dynamic run-time checks:** In this scheme, an application has restricted access to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions or

Table 4.17 | Tools used to defend/protect buffer overflow

<i>Sr. No.</i>	<i>Tool</i>	<i>Brief Description</i>
1	StackGuard	It was released for GCC in 1997 and published at USENIX Security 1998. It is an extension to GCC that provides buffer overflow protection. It was invented by Crispin Cowan. It is a compiler approach for defending programs and systems against “stack-smashing” attacks. These attacks are the most common form of security vulnerability. Programs that have been compiled with StackGuard are largely immune to stack-smashing attack. Whenever vulnerability is exploited, it detects the attack in progress, raises an intrusion alert and halts the victim program.
2	ProPolice	The “stack-smashing protector” or SSP, also known as ProPolice, is an enhancement of the StackGuard concept written and maintained by Hiroaki Etoh of IBM. Its name derives from the word propolis. The stack protection provided by ProPolice is specifically for the C and C++ languages. It is also optionally available in Gentoo Linux with the hardened USE flag.
3	LibSafe	It was released in April 2000 and gained popularity in the Linux community. It does not need access to the source code of the program to be protected. Libsafe protection is system wide and automatically gets attached to the applications. It is based on a middleware software layer that intercepts all function calls made to library functions known to be vulnerable. A substitute version of the corresponding function implements the original function in a way that ensures that any buffer overflows are contained within the current stack frame, which prevents attackers from overwriting the return address and hijacking the control flow of a running program. The real benefit of using libsafe is protection against future attacks on programs not yet known to be vulnerable.

it can ensure that return addresses are not overwritten. One example of such a tool is libsafe. The libsafe library provides a way to secure calls to these functions, even if the function is not available. It makes use of the fact that stack frames are linked together by frame pointers. When a buffer is passed as an argument to any of the unsafe functions, libsafe follows the frame pointers to the correct stack frame. It then checks the distance to the nearest return address and when the function executes, it makes sure that address is not overwritten.

5. **Various tools are used to detect/defend buffer overflow:** See Table 4.17 to know about few such tools.

4.12 Attacks on Wireless Networks

Even when people travel, they still need to work. Thus, work seems to be moving out of the traditional offices into homes, hotels, airport lounges and taxis. The employee is no longer tied to an office location and is, in effect, “boundaryless.” When one talks to the young generation about their lifestyles, one realizes that gone are those days when an “office” conjured up the image of the four walls, set in the formal setting, typical office decor and with all the formality that one can imagine, which may perhaps be difficult for our new generation to appreciate. In the yesteryears, “working” meant leaving home, commuting to the workplace, spending those typical 9 a.m.–6 p.m. in the office and then shutting down the work and commuting back home or wherever that one wished to be after office hours. The “working” and “away from work” were cleanly delineated distinct states that one could be in. Gone are those days and now we are in the era of computing anywhere, anytime! There is no doubt that workforce “mobility” is on the rise (see Box 9.1, Chapter 9).

The following are different types of “mobile workers”:

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes home workers, tele-cottagers and, in some cases, branch workers.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. **Road warrior:** This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels. This type includes the sales and field forces.

Wireless technologies have become increasingly popular in day-to-day business and personal lives. Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs. Wireless networks are generally composed of two basic elements: (a) access points (APs) and (b) other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or “connect” with each other (see Fig. 4.6). APs are connected through physical wiring to a conventional network, and they broadcast signals with which a wireless device can connect.

Wireless access to networks has become very common by now in India – for organizations and for individuals. Many laptop computers have wireless cards preinstalled for the buyer, for example, in India, such cards are provided by TATA Indicom, Reliance and Airtel. There are many hotels and equivalent establishments all over the world (including India) where the rooms are “Wi-Fi enabled.” There is no denying that the ability to enter a network while on the move (working away from home or in other locations that are not routine office locations, working while in hotels, etc.) has great benefits (see Box 4.10 for some interesting facts).

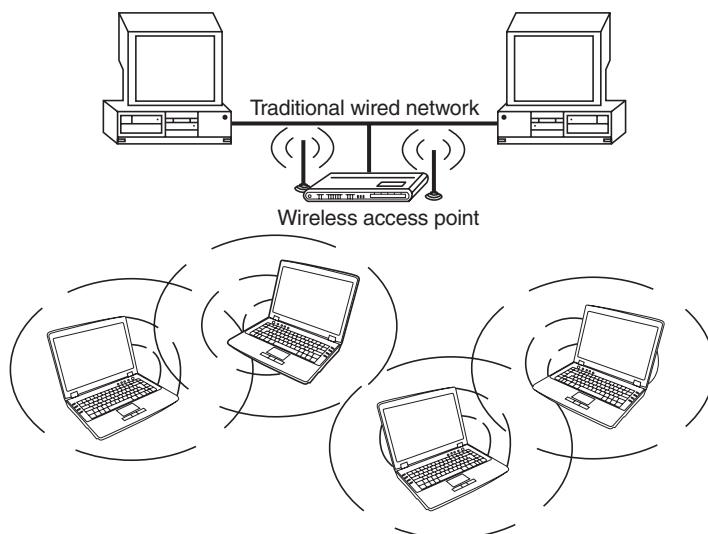


Figure 4.6 | Wireless networks.

Box 4.10 Going Wi-Fi

Start with a laptop computer or other portable device that could benefit from Internet access. Make sure it is wireless. Look for Intel's Centrino sticker or any sign that Wi-Fi is built into the device. If not, you need an external Wi-Fi Personal Computer Memory Card International Association (PCMCIA)-compliant card. Find a public hotspot by searching store windows for stickers that say Wi-Fi Zone, T-Mobile HotSpot or anything indicating a wireless service. Boot up your laptop and login, at home or at a hotel, or get a Wi-Fi router and plug one end into your cable or digital subscriber line (DSL) modem. The router will broadcast the wireless Internet signal in your house and you can sit on the couch and surf the Internet.

Although wireless technology is not new, it is now being used by families who need an easy way to share a fast Internet connection with two or more computers at home. It is helping almost anybody, that is, even the "non-techie," to get Internet access while they buy their daily cup of coffee at a Wi-Fi coffeehouse. This kind of scene is now very common in most Indian metros, including some small cities too.

Cell phones have become indispensable for many who use them to keep track of family members or to call for help in an emergency. Wi-Fi is not there yet, however, the idea of wireless Internet access on every corner is becoming a 24/7 possibility as more companies set up public hotspots. Like cell phones, Wi-Fi is not something you will use every minute, but it can be convenient when you need to check for an E-Mail message or compare the price of an online gift.



Readers may like to visit <http://computer.howstuffworks.com/wifi-quiz.htm> to test fundamental knowledge about wireless networks before going through this section.

Wireless technology is no more buzzword in today's world. Let us understand important components of wireless network, apart from components such as modems, routers, hubs and firewall, which are integral part of any wired network as well as wireless network.

- 802.11 networking standards:** Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6 and 5 GHz frequency bands.
 - 802.11:** It is applicable to WLANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency-hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
 - 802.11a:** It provides 54 Mbps transmission in the 5 GHz band and uses orthogonal frequency-division multiplexing (OFDM) which is more efficient coding technique compared with FHSS and DSSS.
 - 802.11b:** It provides 11 Mbps transmission in the 2.4 GHz band and uses complementary code keying (CCK) modulation to improve speeds. In 1999, ratification was made to the original 802.11 standard, and was termed as 802.11b, which allowed wireless functionality comparable to Ethernet. Although it was being a slowest standard, at the same time being the least expensive, the evolution led to the rapid acceptance of 802.11b across the world as the definitive WLAN technology and known as "Wi-Fi standard."
 - 802.11g:** It provides 54 Mbps transmission in the 2.4 GHz band and the same OFDM coding as 802.11a, hence it is a lot faster than 802.11a and 802.11b.
 - 802.11n:** It is the newest standard available widely and uses multiple-input multiple-output (MIMO) that enabled to improve the speed and range significantly. For example, although

802.11g provides 54 Mbps transmission theoretically, however, it can only achieve 24 Mbps of speed because of network traffic congestion. However, 802.11n can achieve speeds as high as 140 Mbps.

The other important 802 family members are as follows:

- **802.15:** This standard is used for *personal WLANs* and covers a very short range. Hence, it is used for *Bluetooth Technology*.
- **802.16:** It is also known as *WiMax*. It combines the benefits of broadband and wireless, hence it provides high-speed wireless Internet over very long distances and provides access to large areas such as cities. This standard is developed by IEEE working group established in 1999 to develop the standards for *Wireless Metropolitan Area Networks*.

2. Access points: It is also termed as AP. It is a hardware device and/or a software that acts as a central transmitter and receiver of WLAN radio signals. Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.

3. Wi-Fi hotspots: A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants) and are commonly offered facility throughout much of North America and Europe.

- *Free Wi-Fi hotspots:* Wireless Internet service is offered in public areas, free of cost and that too without any authentication. The users will have to enable the wireless on their devices, search for such hotspots and will have to say (*click*) connect. The Internet facility is made available to the user. As the authentication mechanism on the router is disabled, user gets connected to WLAN and cybercriminals get their prey. As, access to free hotspots cannot be controlled, cybersecurity is always questioned. Readers may visit www.hotspot-locations.com to find wireless hotspots into their area. Hotspot locations is the free global hotspot database of wireless access points made available to the general public.
- *Commercial hotspots:* The users are redirected to authentication and online payment to avail the wireless Internet service in public areas. The payment can be made using credit/debit card through payment gateways such as PayPal. Major airports and business hotels are usually charged to avail wireless Internet service. Some Internet service providers offer virtual private network (VPN) as a security feature but found to be an expensive option.

Although the user has been authenticated while connecting to a hotspot, it does not mean that he/she is on the secured communication channel. A “poisoned/rogue hotspot” is termed to be a free public hotspot set up by the cybercriminals, with the objective of sniffing the data sent by the user. They can easily obtain the User IDs (i.e., login names), decipher the passwords and/or other sensitive information by examining packets sent by the user (see Section 7.9, Chapter 7).

4. Service set identifier (SSID): It is the name of 802.11i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other. While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN. It is always advised to turn OFF the broadcast of the SSID, which results in the detected network displaying as an unnamed network and the user would need to manually enter the correct SSID to connect to the network. Hence, it is also advised to set the SSID manually rather than leaving it blank. Moreover, it is important to note that turning off the broadcast of the SSID discourages casual wireless snooping, however, it does not stop an attacker trying to attack the network.

5. Wired equivalence privacy (WEP): Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997. It is

always termed as deprecated security algorithm for IEEE 802.11i WLANs. SSID along with WEP delivers fair amount of secured wireless network.

6. **Wi-Fi protected access (WPA and WPA2):** During 2001, serious weakness in WEP was identified that resulted WEP cracking software(s) being made available to enable cybercriminals to intrude into WLANs. WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. WPA2 is the approved Wi-Fi alliance (www.wi-fi.org) interoperable implementation of 802.11i. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government agencies.
7. **Media access control (MAC):** It is a unique identifier of each node (i.e., each network interfaces) of the network and it is assigned by the manufacturer of a network interface card (NIC) stored in its hardware. MAC address filtering allows only the devices with specific MAC addresses to access the network. The router should be configured stating which addresses are allowed. Although this method appears to be very secure, the attacker can spoof a MAC address, that is, copy the known MAC address to entice the network that the device he/she is using belongs to the network , at the same time it is important to note that, in case you purchase a new device or if any visitors would like to connect to the network, you will need to add the MAC addresses of these new devices to the list of approved addresses.



How to find MAC Address?

Readers may visit www-dcn.fnal.gov/DCG-Docs/mac/ OR www.coffer.com/mac_info/ to know the steps to find the MAC address on the systems running on various operating systems (OS) as well as in case if no OS is installed.

While all this sounds very exciting, it is important to understand that wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into. They are known to use wireless technology to crack into non-wireless networks. Network administrators must be aware of these risks and should stay up to date on any new risks that arise. Users of wireless equipment must be aware of these risks so as to take personal protective measures. As the wireless service technology is getting improved and falling within an easy reach of information technology (IT) as well as non-IT workers, the risks to users of wireless technology have increased exponentially (see Section 9.3.1, Chapter 9).

There were relatively few dangers when wireless technology was first introduced. Although the attackers have no time to latch on to the new technology as wireless was not commonly found in the workplace, however, there are a great number of security risks associated with wireless technology. Some issues are obvious and some are not. At a corporate level, it is the responsibility of the IT department to keep up to date with the types of threats and appropriate countermeasures to deploy. Security threats are growing in the wireless arena. The attackers have learnt that there is much vulnerability in the current wireless protocols, encryption methods and the carelessness and ignorance that exist at the user and corporate IT levels. Cracking methods have become much more sophisticated and innovative with the availability of different tools used to search and hack wireless networks. Cracking has become much easier and more accessible with easy-to-use Windows- and Linux-based tools being made available on the Web at no charge (see Table 4.18).

The overall philosophy behind wired networks vs. wireless networks is “trust.” On a wired network, the hardware is under the direct control of the network administrator, and therefore, the overall attitude toward

Table 4.18 | Tools used for hacking wireless networks

<i>Website</i>	<i>Brief Description</i>
http://www.netstumbler.com/	NetStumbler: This tool is based on Windows OS and easily identifies wireless signals being broadcast within range. It also has ability to determine signal/noise that can be used for site surveys.
http://www.kismetwireless.net/	Kismet: This tool detects and displays SSIDs that are not being broadcast which is very critical in finding wireless networks. NetStumbler do not have this key functional element – ability to display wireless networks that are not broadcasting their SSID.
http://sourceforge.net/projects/airsnort/files/	Airsnort: This tool is very easy and is usually used to sniff and crack WEP keys (http://airsnort.shmoo.com/).
http://wirelessdefence.org/Contents/coWPAttyMain.htm	CowPatty: This tool is used as a brute force tool for cracking WPA-PSK and is considered to be the “New WEP” for home wireless security. This program simply tries a bunch of different options from a dictionary file to see if one ends up matching what is defined as the preshared key.
http://www.wireshark.org/	Wireshark (formerly ethereal): Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff out 802.11 management Beacons and probes, and subsequently could be used as a tool to sniff out non-broadcast SSIDs.

Source: <http://www.ethicalhacker.net/content/view/16/24/> (10 May 10).

the workstations tends to be one of trust. With a wireless network, it is possible that someone could sit in the parking lot with a laptop and access your wireless network. Therefore, the general attitude toward wireless workstations tends to be one of extreme distrust. However, this difference in attitude often causes the same administrators to take extreme positions when it comes to guarding network security. Although they tend to go to extreme lengths at securing a wireless network, at times they almost neglect wired network security. Things to watch out are the following: Are there any unused network jacks or unused switch ports in the office? This is important because if someone was able to sneak into the office and plug a laptop into one of these unused jacks, you may no more have the same level of trust in the hardware on your wired network.

4.12.1 Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access is termed as *wireless cracking*. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

1. **Sniffing:** It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network. Also termed as reconnaissance technique, it gathers the required information about the active/available Wi-Fi networks. The attacker usually installs the sniffer remotely on the victim's system and conducts activities such as
 - Passive scanning of wireless network;
 - detection of SSID;
 - collecting the MAC address;
 - collecting the frames to crack WEP.

2. **Spoofing:** The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage. The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a legitimate network. It causes unsuspecting computers to automatically connect to the spoofed network instead of the real one. The attacker can conduct this activity easily because while setting up a wireless network, the computers no longer need to be informed to access the network; rather they access it automatically as soon as they move within the signal range. This convenient feature is always exploited by the attacker.
 - *MAC address Spoofing:* It is a technique of changing an assigned media access control (MAC) address of a networked device to a different one. This allows the attacker to bypass the access control lists on servers or routers by either hiding a computer on a network or allowing it to impersonate another network device.
 - *IP Spoofing:* It is a process of creating IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. To engage in IP Spoofing, the attacker uses a variety of techniques to find an IP address of a trusted host(s) and then modifies the packet headers so that it appears that the packets are coming from that host, that is, legitimate sender.
 - *Frame Spoofing:* The attacker injects the frames whose content is carefully spoofed and which are valid as per 802.11 specifications. Frames themselves are not authenticated in 802.11 networks and hence when a frame has a spoofed source address, it cannot be detected unless the address is entirely faked/bogus.
3. **Denial of service (DoS):** We have explained this attack in detail in Section 4.9.
4. **Man-in-the-middle attack (MITM):** It refers to the scenario wherein an attacker on host A inserts A between all communications – between hosts X and Y without knowledge of X and Y . All messages sent by X do reach Y but through A and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.
5. **Encryption cracking:** It is always advised that the first step to protect wireless networks is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

4.12.2 Theft of Internet Hours and Wi-Fi-based Frauds and Misuses

Information communication technology (ICT) is within reach of people nowadays and most of the new systems (i.e., computers) are equipped for wireless Internet access as more and more people are opting for Wi-Fi in their homes. Wireless network into homes is becoming common necessity because of lifestyle and availability of inexpensive broadband routers that can be configured easily and/or there is no need to configure these devices at all because of plug-and-play feature. This enables the Internet on the finger tip of home users and in case, unfortunately, he/she visits a malicious webpage, the router is exposed for an attack. Thus, as the networks become stronger and more prevalent, more of the signals are available outside the home of the subscriber, spilling over into neighbor's apartments, hallways and the street. In today's era of high dependency on the Internet for many aspects of our life and given that predators are lurking around as potential cybercriminals, they (criminals) often wonder how they can find out who they are stealing it from so that they can get an idea if that information is safe. According to a study by Jupiter Research, 14% of wireless

network owners have accessed their neighbor's connection.^[36] It appears that more and more people are logging on for free.

Cybercriminals know that they should not steal Internet hours purchased by others but somehow they want to get their work done without paying for the Internet connection and they also want to know if anyone knows how to find out who they are stealing it from. Here is what they are mostly likely to do: (a) they find out the IP address of the router that you are using, (b) open up a command prompt (go to start click on run with; type cmd and press enter) at the command prompt and (c) type this command ipconfig/all and press enter. Look for the default gateway (this is the router); once you see the IP address type the routers IP address into your browser and you can find out some information about who you are stealing Internet from.

An interesting question is whether "stealing" wireless Internet is illegal. We have discussed it under a mini-case in Chapter 11 (in CD) and readers may visit the URL provided in Ref. #13, Additional Useful Web References, Further Reading. Here is one scenario, given that use of laptops is now common place. Suppose you figure out how to connect the laptop to one of the many wireless networks detected on your laptop. Is this illegal? As we shall learn in Chapter 6 the laws vary around the world. However, for the most part, logging and collecting information, such as surfing the Web or checking E-Mail, from wireless networks that are accessible to anyone with a receiver is OK. The act of wardriving is searching for wireless networks by a moving vehicle using a portable computer or PDA.^[37] Readers may visit the URL mentioned in Ref. #3, Video Clips, Further Reading to watch a small video clip on how wardriving is conducted.

Software for wardriving is freely available and can be downloaded from the Internet – to name a few NetStumbler for Windows, Kismet or SWScanner for Linux, and FreeBSD, NetBSD, OpenBSD, DragonFly BSD, Solaris and KisMac for Macintosh. Wardrivers log and collect information from the wireless access points (WAP) they find while driving (see Box 4.11). Think about radio airwaves: as long as you have a radio, listening to a radio station broadcasting where you are driving is free (at least in the US).

Box 4.11 The New "Wars" in the Internet Era!

Basically, the term "wardriving" was derived from the term wardialing from the 1983 film WarGames, which involved searching for computer systems to connect to, using software that dialed numbers sequentially, to see which ones were connected to a fax machine or computer. Subsequently, many related terms came up:

1. **Warwalking:** It is also known as "warjogging" and is similar in nature to wardriving, except that it is done on foot rather than conducted from a moving vehicle. The disadvantages of this approach consist in slower speed of travel (resulting in fewer and more infrequently discovered networks) and the absence of a convenient computing environment. Consequently, hand-held devices, such as Pocket PCs that can perform tasks while one is walking or standing, have predominated in this area. The inclusion of integrated Wi-Fi (rather than a CompactFlash, i.e., CF is a mass storage device format used in portable electronic devices or PCMCIA add-in card) in Dell Axim, Compaq iPAQ and Toshiba pocket PCs in 2002 – and, more recently, an active Nintendo DS and Sony PSP enthusiast community possessing Wi-Fi capabilities on these devices — has expanded the extent of this practice as the newer Smartphones have also integrated Global Positioning System (GPS). Of recent note, the Nokia N770, N800 and N810 Internet Tablets have very good antennas and will pick up nearly anything in the area, even blocks away from the unit.
2. **Warbiking:** Although warbiking is same as wardriving, it involves searching for wireless networks while on a moving bicycle or motorcycle. This activity is facilitated by the mounting of a Wi-Fi-capable device on the vehicle itself.

Box 4.11 The New “Wars” . . . (Continued)

3. **Warkitting:** Warkitting was identified by Tsow, Jakobsson, Yang and Wetzel in 2006. This is a combination of wardriving and rootkitting – an attack in which the wireless access point's configuration or firmware is modified over the wireless connection. This allows the attacker to control all traffic for the victim and may even permit to disable Secure Socket Layer (SSL) by replacing HTML content, when it is being downloaded. The attacker first discovers vulnerable wireless routers through wardriving and/or by retrieving the necessary data from existing Wi-Fi access point databases such as WiGLE (www.wigle.net) or WiFiMaps (www.wifimaps.com) to carry out a warkitting attack.
4. **WAPKitting:** In this attack, external software clutches the control of router's firmware that can be easily accomplished by exploiting open administrative access. WAPkitting can theoretically proceed by more traditional means such as buffer overflow. The ability to install arbitrary control software on a wireless router opens unlimited possibilities to an attacker.
5. **WAPjacking:** This type of attack is very similar to DNS poisoning attacks. It changes the settings of existing firmware that helps an attacker to engage in malicious configuration of firmware settings; however, it makes no modification to the firmware itself, that is, allow connections to be hijacked and/or rerouted without the user's knowledge. WAPjacking is less powerful attack compared to WAPkitting.

WAPkitting and WAPjacking are independent of the means of infection, and specify the relative modifications done to a WAP upon corruption. Warkitting, on the other hand, does not specify the type of WAP alteration, but it does relate to how infection occurs.

Source: <http://en.wikipedia.org/wiki/Wardriving> (31 May 2010).

Be careful with use of WAPs; when you are using a WAP to gain access to computer on a network, be aware of the local laws/legislations where you are doing it because things can become dangerous from security and privacy as well legal perspective. Maybe if corporations were not in such a hurry to release this technology and thought about it more thoroughly, they would not have to deal with security breaches and creating superior protection for their own systems. The moral of the story is that you must secure your network.

4.12.3 How to Secure the Wireless Networks

Nowadays, security features of Wi-Fi networking products are not that time-consuming and non-intuitive; however, they are still ignored, especially, by home users. Although following summarized steps will help to improve and strengthen the security of wireless network, see Table 4.19 to know the available tools to monitor and protect the wireless networks:

1. Change the default settings of all the equipments/components of wireless network (e.g., IP address/user IDs/administrator passwords, etc.).
2. Enable WPA/WEP encryption.
3. Change the default SSID.
4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the features that are not used in the AP (e.g., printing/music support).
8. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
9. Connect only to secured wireless network (i.e., do not autoconnect to open Wi-Fi hotspots).
10. Upgrade router's firmware periodically.

Table 4.19 | Tools to protect wireless network

<i>Website</i>	<i>Brief Description</i>
http://www.zamzom.com/	Zamzom Wireless Network Tool: New freeware tool helps to protect wireless networks and maintain computer security, detects all computer names, Mac and IP addresses utilizing a single wireless network, reveals all computers – both authorized and unauthorized – who have access to any given wireless network. Thus, it helps users to take vital steps toward securing their wireless networks and acts as a measure that should not be overlooked or skipped.
http://www.airdefense.net/	AirDefense Guard: The tool provides advanced intrusion detection for wireless LANs and is based on signature analysis, policy deviation, protocol assessment policy deviation and statistically anomalous behavior. AirDefense detects responds to: <ul style="list-style-type: none"> • Denial-of-service (DoS) attacks; • man-in-the-middle attacks; • identity theft.
http://www.loud-fat-bloke.co.uk/tools.html	Wireless Intrusion Detection System (WIDZ): This is an intrusion detection for wireless LANs for 802.11. It guards APs and monitors local frequencies for potentially malevolent activity. It can detect scans, association floods and bogus APs, and it can easily be integrated with other products such as SNORT or Realsecure.
http://www.dachb0den.com/projects/bsd-airtools.html	BSD-Airtools: This tool provides a complete toolset for wireless auditing (802.11b). It contains AP detection application, Dstumbler – similar to Netstumbler. It can be used to detect wireless access points and connected nodes, view signal-to-noise graphs, and interactively scroll through scanned APs and view statistics for each. It also contains a BSD-based WEP cracking application (called as Dweputils).
http://wifi.google.com/	Google Secure Access: Google Wi-Fi is a free wireless Internet service offered to the city of Mountain View (California, USA). With your Wi-Fi-enabled device and a Google Account, one can go online for free by accessing the network name “GoogleWi-Fi,” which is secured by Google’s virtual private network (VPN). Google Secure Access encrypts the Internet traffic and sends it through Google’s servers on the Internet.

11. Assign static IP addresses to devices.
12. Enable firewalls on each computer and the router.
13. Position the router or AP safely.
14. Turn off the network during extended periods when not in use.
15. Periodic and regular monitor wireless network security.

SUMMARY

When information systems are the target of offense, the criminal's goal is to steal information from, or cause damage to, a computer, computer system or computer network. The perpetrators range from teenagers (script kiddies/cyberjoyriders) to organized crime operators and international terrorists.

A computer can be the target of offense; tools may be used in an offense, or may contain evidence of an offense. An understanding of different uses of a computer will provide foundation of the application of the criminal statutes.

The computing technology may also be a tool of an offense. The criminal uses the computer to commit a traditional crime, such as counterfeiting. For example, a counterfeiter that used to engrave plates to create the counterfeit currency can now use sophisticated graphic computers with advanced color printers.

The criminals/attackers have in-depth knowledge about the technology and can use traditional methods/techniques or sophisticated means such as hacking tools to break into the systems. Everybody has to take care of their own systems and this should not be left over to any one person/group of persons (i.e., System Administrator, Chief Information Security Officer). Many scenarios and case illustrations are provided in Chapter 11 (in CD) explaining different

techniques used in cyberattacks. Everybody should follow **R.U.N.S.A.F.E. guidelines:**

1. Refuse to download/install/execute any unknown utilities/tools.
2. Update vital utilities/tools (e.g., OS, antivirus, anti-Spywares, firewalls) regularly.
3. Nullify unnecessary risks.
4. Safeguard own user ID and password.
5. Assure sufficient resources to take care of own systems appropriately.
6. Face insecurity (i.e., what and how much to secure is always a question!).
7. Everybody should do their own job sincerely (i.e., information security is everybody's responsibility similar to "charity begins at home!").

REVIEW QUESTIONS

1. What are the different phases during the attack on the network?
2. What is the difference between proxy server and an anonymizer?
3. What are the different ways of password cracking?
4. How can keyloggers be used to commit a cybercrime?
5. What is the difference between a virus and a worm?
6. What is virus hoax?
7. What is the difference between Trojan Horses and backdoors?
8. What is the difference between steganography and cryptography?
9. Are countermeasures employed against steganography? Explain.
10. What is the difference between DoS and DDoS?
11. What is SQL injection and what are the different countermeasures to prevent the attack?
12. What is Blind SQL injection attack? Can it be prevented?
13. What are different buffer overflow attacks?
14. What are the different components of wireless network?
15. What is the difference between WEP and WPA2?
16. How can wireless networks be comprised?
17. What is the difference between WAPkitting and WAPjacking?

REFERENCES

- [1] To know more about anonymizer, visit: <http://en.wikipedia.org/wiki/Anonymizer> (6 September 2009).
- [2] To know more about Google cookie, visit: <http://www.google-watch.org/bigbro.html> (2 October 2009).
- [3] To know more about DART cookie, visit: <http://www.doubleclick.com/privacy/faq.aspx> (2 October 2009).
- [4] To know more on G-Zapper, visit: <http://www.dummysoftware.com/gzapper.html> (2 October 2009).
- [5] To know more on Phishing, visit: <http://computer.howstuffworks.com/phishing.htm> (29 May 10).
- [6] To know more about password, visit: http://en.wikipedia.org/wiki/Password_cracking (2 October 2009).

- [7] To know more about MITM attacks, visit: http://en.wikipedia.org/wiki/Man-in-the-middle_attack (2 October 2009).
- [8] To know more about strength of a password, visit: <http://www.microsoft.com/protect/fraud/passwords/checker.aspx> (2 October 2009).
- [9] To know more about keyloggers, visit: http://en.wikipedia.org/wiki/Keystroke_logging (4 October 2009).
- [10] To know more about software keyloggers, visit: http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci962518,00.html (4 October 2009).
- [11] To know more about antikeylogger, visit: <http://www.anti-keyloggers.com/products.html> (4 October 2009).
- [12] To know more about Spyware, visit: <http://en.wikipedia.org/wiki/Spyware> (5 October 2009).
- [13] To know more about malware, visit: <http://en.wikipedia.org/wiki/Malware> (5 October 2009).
- [14] To know more about Trojan Horses visit: [http://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing)) (8 October 2009).
- [15] To know more about rootkit, visit: <http://en.wikipedia.org/wiki/Rootkit> (8 October 2009).
- [16] To know more about backdoor, visit: [http://en.wikipedia.org/wiki/Backdoor_\(computing\)](http://en.wikipedia.org/wiki/Backdoor_(computing)) (8 October 2009).
- [17] To know more about viruses, worms and Trojans, visit: http://en.wikipedia.org/wiki/Computer_virus (1 March 2010).
- [18] To understand difference between computer virus and worm, visit: http://www.diffen.com/difference/Computer_Virus_vs_Computer_Worm (1 March 2010).
- [19] To know types of viruses, visit: <http://www.spamlaws.com/virus-types.html> (1 March 2010).
- [20] To know more on worm, visit: http://en.wikipedia.org/wiki/Computer_worm (1 March 2010).
- [21] To understand various aspects of viruses, visit: <http://www.kernelthread.com/publications/security/vunix.html> (1 March 2010).
- [22] To know more about Trojan Horse, visit: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html (11 January 2010).
- [23] To know more about threats by Trojan Horses, visit: <http://www.techsupportalert.com/best-free-trojan-scanner-trojan-remover.htm> (11 January 2010).
- [24] To know more about backdoor, visit: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci962304,00.html (10 January 2010).
- [25] To know more about what a backdoor does, visit: <http://www.2-spyware.com/backdoors-removal> (10 January 2010).
- [26] To know more about SAP backdoors, visit: <http://blog.c22.cc/2010/04/14/blackhat-europe-sap-backdoors-a-ghost-at-the-heart-of-your-business-4/> (29 May 2010).
- [27] To know more about what is P2P network, visit: <http://en.wikipedia.org/wiki/Peer-to-peer> (29 May 2010).
- [28] To understand different levels of P2P networks, visit: <http://disco.ethz.ch/theses/ss05/freenet.pdf> (29 May 2010).
- [29] To know more about steganography, visit: <http://en.wikipedia.org/wiki/Steganography> (11 October 2009).
- [30] Visit New York Times reports usage of steganography at: <http://en.wikipedia.org/wiki/Steganography> (11 October 2009).
- [31] To know more about DoS: Teardrop attack, visit: http://en.wikipedia.org/wiki/Denial-of-service_attack (11 May 2010).
- [32] To know more about DoS: Nuke attack, visit: http://wapedia.mobi/en/Denial_of_Service (11 May 2010).

- [33] To know how to prevent DoS attacks, visit: http://www.cert.org/tech_tips/denial_of_service.html#4 (11 May 2010).
- [34] To know more about SQL injection and Blind SQL injection attacks, visit: http://en.wikipedia.org/wiki/SQL_injection (11 May 2010).
- [35] To know more about buffer overflow: NOOP, visit: http://en.wikipedia.org/wiki/Buffer_overflow (11 May 2010).
- [36] To know more about wireless network – frauds and misuses, visit: <http://www.88450.com/redirect.php?tid=55751&goto=lastpost> (11 May 2010).
- [37] To know more about wardriving, visit: http://en.wikipedia.org/wiki/War_driving (11 May 2010).

FURTHER READING

Additional Useful Web References

1. To know how anonymizers work, visit: http://www.livinginternet.com/i/is_anon_work.htm (6 September 2009).
2. To know more about anonymizer FAQs, visit: <http://www.anonymizer.com/company/about/anonymizer-faq.html> (6 September 2009).
3. To understand a framework for classifying denial-of-service attacks, visit: http://isi.edu/div7/publication_files/tr-569.pdf (30 May 2010).
4. To understand wireshark frequently asked questions, visit: <http://www.wireshark.org/faq.html> (30 May 2010).
5. To understand classification of DoS attack, visit: <http://www.technospot.net/blogs/types-of-dos-attacks-and-introduction-to-ddos/> (30 May 2010).
6. To understand types of DoS attacks, visit: <http://www-rp.lip6.fr/~blegrand/cours/MIAIF/secu1.pdf> (30 May 2010). <http://www.topbits.com/denial-of-service-dos-attacks.html> (30 May 2010).
7. To understand blind SQL injection, visit: http://www.net-security.org/dl/articles/Blind_SQLInjection.pdf (30 May 2010).
8. To know more about SQL injection protection, visit: http://www.owasp.org/images/7/7d/Advanced_Topics_on_SQL_Injection_Protection.ppt (30 May 2010).

9. To know how to protect from injection attacks in ASP.NET, visit: <http://msdn.microsoft.com/en-us/library/ff647397.aspx> (30 May 2010).
10. To know more about buffer overflow attacks and their countermeasures, visit: <http://www.linuxjournal.com/article/6701?page=0,0> (30 May 2010).
11. To know more about article *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*, visit: <http://www.ece.cmu.edu/~adrian/630-f04/readings/cowan-vulnerability.pdf> (30 May 2010).
12. Stealing your neighbor's Net, visit: http://money.cnn.com/2005/08/08/technology/personaltech/internet_piracy/index.htm (30 May 2010).
13. Is "Stealing" Wireless Internet Illegal?, visit: <http://journalism.nyu.edu/pubzone/wewant-media/node/10> (30 May 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Kimberly, G. (2007) *CEH: Official Certified Ethical Hacker Review Guide*, Wiley Publishing, Inc., IN, USA.
3. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

Video Clips

1. To know more about *Demonstration of Scareware*, visit: <http://www.youtube.com/watch?v=nRgkFt0NLsw> (16 February 2010).
2. To know more about *Crime: The Real Internet Security Problem*, visit: <http://www.youtube.com/watch?v=rZ1rkIy0dMM> (16 February 2010).
3. To know more on how wardriving is conducted, visit: http://www.metacafe.com/watch/1708061/i_quit_movie_scene_24_stealing_internet_access/ (16 September 2009).

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, C, D, E, J, L. These are provided in the companion CD.

5

Phishing and Identity Theft

Learning Objectives

After reading this chapter, you will be able to:

- Learn about Phishing and its related techniques.
 - Understand different methods of Phishing.
 - Get an overview about 3Ps of cybercrime (Phishing, Pharming and Phoraging).
 - Understand what Spear Phishing is and how to avoid being victim of Spear Phishing.
 - Get an overview of “whaling.”
 - Learn about identity (ID) theft and understand ID theft as a major threat to businesses.
 - Understand “myths and facts” about ID theft.
 - Understand different types of ID thefts.
 - Learn about different techniques of ID theft.
 - Understand about countermeasures for ID theft.
-

5.1 Introduction

Chapter 4 has provided an insight on how different methods and tools are used to conduct cyberoffenses and Phishing was introduced in Chapter 4 as one of the methods toward enticing netizens to reveal their personal information that can be used for identity (ID) theft. ID theft involves unauthorized access to personal data. Section 66C of the Indian IT Act states that *“whosoever fraudulently make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.”* Section 66D of the Indian IT Act states that *“whoever, by means for any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable for fine which extend to one lakh rupees.”* “Phishing” is the use of social engineering tactics to trick users into revealing confidential information.

Phishing has become a universal phenomenon and a major threat worldwide that affects not only individuals but also all industries and businesses that have an online presence and do online transactions over the Internet. Phishing is equal parts of technology and psychology – resorted to a systematic way to exploit netizens, not only by individual attackers but also by organized criminal groups.

The statistics about Phishing attacks/scams proves *Phishing* to be a dangerous enemy among all the methods/techniques discussed in Chapter 4, because the prime objective behind these attacks is ID theft.

1. The world Phishing map available at www.avira.com^[1] illustrates that the most Phishing attacks are on the rise in Asia, Europe and North America. The virus laboratory at Avira is constantly monitoring the evolution of E-Mail Phishing across the globe.

2. The graphical illustrations available on www.m86security.com^[2] exhibit the following facts:
 - Monitoring of continent of origin from where Phishing E-Mails are sent. Europe is the dominant source of Phishing E-Mails.
 - Facebook, HSBC, Paypal and Bank of America are the most targeted organizations in Phishing attacks.
 - US, India and China are the most targeted countries to launch Phishing attacks.
3. The Phishing attacks are monitored on daily basis and displayed on www.phishtank.com.^[3] The statistics displayed are “phishes verified as valid” and “suspected phishes submitted.” It is important to note that more than five million E-Mails are identified as “verified and valid” phished E-Mails almost everyday.
4. According to May 2009 Phishing Monthly Report compiled by Symantec Security Response Anti-Fraud Team^[4].
 - Total 3,650 non-English Phishing websites were recorded in the month of May 2009 and out of these, French language Phishing sites were the most frequently recorded followed by websites in Italian and Chinese languages.
 - Phishing URLs are categorized based on the top-level domains (TLDs). The most used TLDs in Phishing websites during the month of May 2009 were “.com,” “.net” and “.org” comprising 50%, 9% and 5%, respectively.
5. Phishing Activity Trends Report of Q4-2009^[5] published by Anti-Phishing Working Group (APWG, see Box 5.1) states the Phishing attack trends and statistics for the quarter. It is important to note that:
 - Financial organizations, payment services and auction websites are ranked as the most targeted industry.
 - Port 80 is found to be the most popular port in use followed by Port 443 and Port 8080 among all the phishing attacks.

This chapter aims to lay the foundation to understand Phishing and different techniques and methods of Phishing attacks. One needs to wear *HAT* and put oneself into the *SHOES* of the phisher (scammers who perpetrate Phishing scams) to understand Phishing. Phishers are also getting educated and attempt new methods and techniques to victimize netizens. Therefore, it is crucial to discuss about countermeasures to avoid becoming victim of Phishing attacks, which we have discussed at the end of this chapter. “Phishing”

Box 5.1 APWG (Anti-Phishing Working Group)

The Anti-Phishing Working Group (APWG) – www.antiphishing.org – is an international consortium, founded in 2003 by David Jevans, to bring security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies together, who are affected by Phishing attacks.

APWG has more than 3,200+ members from more than 1,700 organizations and agencies across the globe. To name a few, member organizations are leading security companies such as BitDefender, Symantec, McAfee, VeriSign and IronKey. ING Group, VISA, Mastercard and the American Bankers Association are the members from financial industry.

APWG is focused on eliminating identity theft that results from the growing attacks/scams of Phishing and E-Mail Spoofing. APWG provides a platform to discuss Phishing issues, define the scope of the Phishing problem in terms of costs and share information about best practices to eliminate these attacks/scams.

Source: http://en.wikipedia.org/wiki/Anti-Phishing_Working_Group (9 June 2010).

attacks and “ID theft” both have an impact on individual’s “privacy.” Detailed discussion about “privacy” from all perspectives can be found in Ref. #2, Books, Further Reading.

5.2 Phishing



The word Phishing comes from the analogy that Internet scammers are using E-Mail lures to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords from unsuspecting AOL users. As hackers have a tendency of replacing “f” with “ph” the term Phishing came into being.

Source: <http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp> (9 June 2010).

Let us take a look at some definitions of the term “Phishing.”

1. **Wikipedia:** It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.^[6]
2. **Webopedia:** It is an act of sending an E-Mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for ID theft. The E-Mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security and bank account numbers that the legitimate organization already has. The website, however, is bogus and set up only to steal the users' information.^[7]
3. **TechEncyclopedia:** It is a scam to steal valuable information such as credit card and social security numbers (SSN), user IDs and passwords. It is also known as “brand Spoofing.” An official-looking E-Mail is sent to potential victims pretending to be from their bank or retail establishment. E-Mails can be sent to people on selected lists or any list, expecting that some percentage of recipients will actually have an account with the organization.^[8]

In summary, Phishing is a type of *deception designed to steal your identity* (i.e., a kind of ID theft fraud). In Phishing schemes, the phisher tries to get the user to disclose valuable personal data – such as credit card numbers, passwords, account data or other information – by convincing the user to provide it under false pretenses. E-Mail is the popular medium used in the Phishing attacks and such E-Mails are also called as Spams; however, not all E-Mails are spam E-Mails. It is important to understand these types of E-Mails with which we deal everyday. We will discuss two such E-Mails: (A) Spam E-Mails (introduced in Section 1.5.2, Chapter 1) and (B) hoax E-Mails.

A. Spam E-Mails

Also known as “junk E-Mails” they involve nearly identical messages sent to numerous recipients. Spam E-Mails have steadily grown since the early 1990s. Botnets (explained in Chapters 1 and 2), networks of virus-infected computers, are used to send about 80% of Spam. Types of Spam E-Mails are as follows:

1. **Unsolicited bulk E-Mail (UBE):** It is *synonym for SPAM* (introduced in Box 1.5, Chapter 1) – unsolicited E-Mail sent in large quantities (see Box 5.2).
2. **Unsolicited commercial E-Mail (UCE):** Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising. See Box 5.3 to know more about US Act on Spam mails.

Box 5.2 SPAMBOTS

SPAMBOT is an automated computer program and/or a script developed, mostly into "C" programming language, to send Spam mails. SPAMBOTS gather the E-Mail addresses from the Internet, to build mailing lists to send unsolicited E-Mail. SPAMBOTS are also known as web crawlers, as they gather E-Mail addresses from numerous websites, chatroom conversations, newsgroups and special-interest group (SIG) postings. SPAMBOT begins its scan on a webpage and search for two things: (a) hyperlinks and (b) E-Mail addresses. It gathers and stores E-Mail addresses and crawls (i.e., follows) through each hyperlink to a new page to gather E-Mail addresses.

The term SPAMBOT is also sometimes used with reference to a program designed to prevent Spam to reach the subscribers of an Internet service provider (ISP). Such programs are called *E-Mail blockers* or *filters*. Such E-Mail blocker and/or filter, occasionally, may block a legitimate E-Mail message which could not be delivered to the intended recipient. This can be avoided by allowing each subscriber to generate a whitelist of specific E-Mail addresses the blocker should pass.

Source: <http://en.wikipedia.org/wiki/Spambot> (26 July 2010).

Box 5.3 CAN-SPAM Act

The CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108-187, was S.877 of the 108th US Congress), signed into law by President George W. Bush on 16 December 2003, establishes the United States' first national standards for the sending of commercial E-Mail and requires the Federal Trade Commission (FTC) to enforce its provisions. The acronym CAN-SPAM derives from the bill's full name: Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003. This can also be a play on the usual term for unsolicited E-Mail of this type of Spam. The bill was sponsored in Congress by Senators Conrad Burns and Ron Wyden.

Visit the weblink <http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm> to know more about this act (see Fig. 1.13, Chapter 1 and Section "Spam Laws" under Section 6.2.2, Chapter 6).

The CAN-SPAM Act is commonly referred to as the "You-Can-Spam" Act because the bill explicitly legalizes most E-Mail Spam. In particular, it does not require E-Mailers to get permission before they send marketing messages. It also prevents states from enacting stronger anti-Spam protections, and prohibits individuals who receive Spam from suing spammers. The Act has been largely unenforced, despite a letter to the FTC from Senator Burns, who noted that "Enforcement is a key factor with regard to the CAN-SPAM legislation." In 2004, less than 1% of Spam was complied with the CAN-SPAM Act of 2003 (see Example 16, Section 11.2.16, Chapter 11 in CD).

Source: http://en.wikipedia.org/wiki/CAN-SPAM_Act_of_2003 (9 June 2010).

Spam E-Mails proved to be a popular medium for phishers to scam users to enter personal information on fake websites using E-Mail forged to look like as if it is from a bank or other organizations such as:^[9]

1. **HSBC, Santander, CommonWealth Bank:** International Banks having large customer base, phishers always dive deep in such ocean to attempt to hook the fish.
2. **eBay:** It is a popular auction site, often mimicked to gain personal information.
3. **Amazon:** It was the top brand to be exploited by phishers till July 2009.
4. **Facebook:** Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mail. One can reduce chances of being victim of Phising attack by using the services – security settings to enable contact and E-Mail details as private. In Chapter 7 (Section 7.14) security and privacy threats from social networking sites are discussed.

The E-Mail will usually ask the user to provide valuable information about himself/herself or to “verify” information that the user may have provided in the past while registering for online account. To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics:^[10]

1. **Names of legitimate organizations:** Instead of creating a phony company from scratch, the phisher might use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-Mail.
2. **“From” a real employee:** Real name of an official, who actually works for the organization, will appear in the “from” line or the text of the message (or both). This way, if a user contacts the organization to confirm whether “Rajeev Arora” truly is “Vice President of Marketing” then the user gets a positive response and feels assured.
3. **URLs that “look right”:** The E-Mail might contain a URL (i.e., weblink) which seems to be legitimate website wherein user can enter the information the phisher would like to steal. However, in reality the website will be a quickly cobbled copycat – a “spoofed” website that looks like the real thing, that is, legitimate website. In some cases, the link might lead to selected pages of a legitimate website – such as the real company's actual privacy policy or legal disclaimer. We will discuss more on this in Section 5.2.2.
4. **Urgent messages:** Creating a fear to trigger a response is very common in Phishing attacks – the E-Mails warn that failure to respond will result in no longer having access to the account or E-Mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.

Here are a few examples of phrases used to entice the user to take the action.

1. **“Verify your account”:** The organization will never ask the user to send passwords, login names, permanent account numbers (PANs) or SSNs and other personal information through E-Mail. For example, if you receive an E-Mail message from Microsoft asking you to update your credit card information, do not respond without any confirmation with Microsoft authorities – this is a perfect example of Phishing attack.
2. **“You have won the lottery”:** The lottery scam is a common Phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work on your part. The lottery scam often includes references to big companies, for example, Microsoft. There is no Microsoft lottery. It is observed that most of the phished E-Mails display the name of the agencies/companies situated in Great Britain and hence it is extremely important for netizens to confirm/verify the authenticity of such E-Mails before sending any response.
 - If any E-Mail is received displaying “You have won the lottery in Great Britain,” confirm it on www.gamblingcommission.gov.uk
 - If any E-Mail is received displaying your selection for any job into Great Britain, confirm/verify the details of the organization on www.companieshouse.gov.uk or on <http://www.upmystreet.com/local/uk.html>
3. **“If you don't respond within 48 hours, your account will be closed”:** These messages convey a sense of urgency so that you will respond immediately without thinking. A Phishing E-Mail message might even claim that your response is required because your account might have been compromised.



Visit the weblinks mentioned below to undergo a quiz to test your Phishing IQ:

1. www.sonicwall.com/Phishing/index.html,
2. <http://www.washingtonpost.com/wp-srv/technology/articles/phishingtest.html>

Although Phishing is categorized as Spam, it also differs from Spam. Spam attempts to sell a product or service whereas a phished E-Mail seems to be sent by a legitimate organization/institute. As Phishing and legitimate messages appear to be similar, techniques that are applied to Spam messages cannot be applied naively to Phishing messages. The purpose of a phished E-Mail is to obtain sensitive personal information about a netizen/Internet user and to do so E-Mail needs to deceive the intended recipient into believing that it is from a legitimate organization/institute. As a form of deception, a Phishing E-Mail contains no useful information for the intended recipient and thus falls under the category of Spam.

Let us understand the ways to reduce the amount of Spam E-Mails we receive.^[11]

1. Share personal E-Mail address with limited people and/or on public websites – the more it is exposed to the public, the more Spam E-Mails will be received.
2. Never reply or open any Spam E-Mails. Any spam E-Mails that are opened or replied to inform the phishers not only about your existence but also about validity of your E-Mail address.
3. Disguise the E-Mail address on public website or groups by spelling out the sign “@” and the DOT (.); for example, *RajeevATgmailDOTcom*. This usually prohibits phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.
4. Use alternate E-Mail addresses to register for any personal or shopping website. Never ever use business E-Mail addresses for these sites but rather use E-Mail addresses that are free from Yahoo, Hotmail or Gmail.
5. Do not forward any E-Mails from unknown recipients.
6. Make a habit to preview an E-Mail (an option available in an E-Mail program) before opening it.
7. Never use E-Mail address as the screen name in chat groups or rooms.
8. Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.

B. Hoax E-Mails

These are deliberate attempt to deceive or trick a user into believing or accepting that something is real, when the hoaxter (the person or group creating the hoax) knows it is false.^[12] Hoax E-Mails may or may not be Spam E-Mails. It is difficult sometimes to recognize whether an E-Mail is a “Spam” or a “hoax.” The websites mentioned below can be used to check the validity of such “hoax” E-Mails – for example, chain E-Mails. In Chapter 11 in CD, Example 16 illustrates CAN-SPAM Act Violation through E-Mail Stock Fraud (see Section 11.2.16).

1. **www.breakthechain.org:** This website contains a huge database of chain E-Mails, like we discussed, the phisher sends to entice the netizens to respond to such E-Mails (e.g., from “lottery schemes” to “your wish will come true” E-Mails). One can search the subject line of such an E-Mail or a couple of key words on this website to know whether it is a Spam E-Mail or a legitimate E-Mail.
2. **www.hoaxbusters.org:** This is an excellent website containing a large database of common Internet hoaxes. It is maintained by the Computer Incident Advisory Capability, which is a division of the US Department of Energy. Hoaxbusters contains information almost about every scam, legend and frivolous warning that exists on the Internet. For example, mail with the subject as “Breaking News” may contain the text as “Barack Obama refused to be the president of the US” and will end with the E-Mail signature as “CNN.”



Visit the weblink to learn few examples of hoax E-Mails at <http://www.westpac.com.au/security/fraud-and-scams/latest-hoax-email-examples>

5.2.1 Methods of Phishing

Let us understand the most frequent methods used by the phishers^[13] to entice the netizens to reveal their personal information on the Internet.

1. **Dragnet:** This method involves the use of spammed E-Mails, bearing falsified corporate identification (e.g., corporate names, logos and trademarks), which are addressed to a large group of people (e.g., customers of a particular financial institution or members of a particular auction site) to websites or pop-up windows with similarly falsified identification. Dragnet phishers do not identify specific prospective victims in advance. Instead, they rely on false information included in an E-Mail to trigger an immediate response by victims – typically, clicking on links in the body of the E-Mail to take the victims to the websites or pop-up windows where they are requested to enter bank or credit card account data or other personal data.
2. **Rod-and-reel:** In this method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data. For example, on the phony webpage, availability of similar item for a better price (i.e., cheaper price) is displayed which the victims may be searching for and upon visiting the webpage, victims were asked for personal information such as name, bank account numbers and passwords, before confirming that the “sale” and the information is available to the phisher easily.
3. **Lobsterpot:** This method focuses upon use of spoofed websites. It consists of creating of bogus/phony websites, similar to legitimate corporate ones, targeting a narrowly defined class of victims, which is likely to seek out. See Box 5.4 to know more about other attacks launched on the legitimate websites to grab the user’s personal information. These attacks are also known as “content injection Phishing.” Visit <http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx> to see the example of a deceptive URL address linking to a scam website. The phisher places a weblink into an E-Mail message to make it look more legitimate and actually takes the victim to a phony scam site, which appears to be a legitimate website or possibly a pop-up window that looks exactly like the official site. These fake sites are also called “spoofed” websites. Once the netizen is into one of these spoofed sites, he/she might unwittingly send personal information to the con artists. Then they often use your information to purchase goods, apply for a new credit card or otherwise steal your identity. Box 5.5 explains Phishing vis-à-vis Spoofing.
4. **Gillnet:** This technique relies far less on social engineering techniques and phishers introduce Malicious Code into E-Mails and websites. They can, for example, misuse browser functionality by injecting hostile content into another site’s pop-up window. Merely by opening a particular E-Mail, or browsing a particular website, netizens may have a Trojan Horse introduced into their systems. In some cases, the Malicious Code will change settings in user’s systems so that users who want to visit legitimate banking websites will be redirected to a look alike Phishing site. In other cases, the Malicious Code will record user’s keystrokes and passwords when they visit legitimate banking sites, and then transmit those data to phishers for later illegal access to users’ financial accounts. We will discuss more on this in the next section while understanding Phishing techniques used by phishers.

Box 5.4 Website Spoofing, XSS and XSRF

Website Spoofing: It is the act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization. Normally, the website will adopt the design of the target website and it sometimes has a similar URL.^[14]

Box 5.4 Website Spoofing, . . . (Continued)

Cross-site scripting (XSS): XSS^[15] is a type of computer security vulnerability typically found in web applications that enable malicious attackers to inject client-side script into webpages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

1. John often visits a particular website that is hosted by Bill. Bill's website allows John to log in with a username/password pair and store sensitive information such as billing information.
2. Bruce observes that Bill's website contains a reflected XSS vulnerability.
3. Bruce crafts a URL to exploit the vulnerability, and sends John an E-Mail, enticing him to click on a link for the URL under false pretenses.
4. John visits the URL provided by Bruce while logged into Bill's website.
5. The malicious script embedded in the URL executes in John's browser, as if it came directly from Bill's server. The script can be used to send John's session cookie to Bruce. Bruce can then use the session cookie to steal sensitive information available to John (authentication credentials, billing info, etc.) without John's knowledge.

Cascading style sheets is referred to as CSS, hence cross-sites scripting is referred to as XSS. CSS is a style sheet language used to describe the presentation semantics (i.e., look and formatting) of a document written in a markup language such as HTML and XHTML.

Cross-site request forgery (XSRF): XSRF^[16] is also known as a one-click attack or session riding (abbreviated as CSRF or XSRF) and is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has on a particular site, CSRF exploits the trust that a site has in a user's browser.

1. Bill might be browsing a chat forum where another user, Bruce, has posted a message.
2. Bruce has crafted an HTML image element that references a script on Bill's bank's website.
3. In case Bill's bank keeps his authentication information in a cookie, and if the cookie has not expired, then the attempt by Bill's browser to load the image will submit the withdrawal form with his cookie, thus authorizing a transaction without Bill's approval.
4. This case displays Bill's web browser that is confused into misusing Bill's authority at Bruce's direction.

Box 5.5 Phishing vis-à-vis Spoofing

1. Phishing is used to get the victim to reveal valuable (or at times invaluable) information about him/her. Phishers would use Spoofing to create a fake E-Mail.
2. Spoofing is not intended to steal information but to actually make the victim do something for phishers.
3. Phishing may, at times, require Spoofing to entice the victim into revealing the information but Spoofing does not always necessarily result in Phishing someone else's account.

The Combined Attack – Phishing and Spoofing

Phisher sends an E-Mail, during Income Tax return filing period, from an official looking IT (Income Tax) account which is spoofed. The E-Mail would contain URL to download a new tax form that was recently issued. Once the victim clicks the URL, a "virus cum Trojan Horse" is downloaded to the victim's system. The IT Form may seem official, but like a Trojan Horse, the payload (explained in Section 2.7, Chapter 2) has already been delivered. The virus lies in wait, logging the actions of the victim. Once the victim inputs certain keywords, like bank names, credit card names, social networking websites and so forth, it logs the site and the passwords used. Those results are flagged and sent to the phisher. The virus could then gather the user's E-Mail contacts and send a fake E-Mail to them as well, containing the virus. The phisher now has gained the required personal information as well as virus was sent, downloaded and spread to entice other netizens.

5.2.2 Phishing Techniques

In this section we will discuss common ways, the techniques^[17] used by phishers to launch Phishing attacks.

1. **URL (weblink) manipulation:** URLs are the weblinks (i.e., Internet addresses) that direct the netizens/users to a specific website. In Phishing attack, these URLs are usually supplied as misspelled, for example, instead of www.abcbank.com, URL is provided as www.abcbank1.com. Phishers use Lobsterpot method of Phishing and make the difference of one or two letters in the URLs, which is ignored by netizens. This makes a big difference and it directs users to a fake/bogus website or a webpage. See Box 5.6 to know about an advanced Phishing attack known as homograph attack.
2. **Filter evasion:** This technique use graphics (i.e., images) instead of text to obviate from netting such E-Mails by anti-Phishing filters. Normally, these filters are inbuilt into the web browsers. For example,
 - Internet Explorer version 7 has inbuilt “Microsoft phishing filter.” One can enable it during the installation or it can be enabled post-installation. It is important to note that it is *not enabled* by default.
 - Firefox 2.0 and above has inbuilt “Google Phishing filter,” duly licensed from Google. It is enabled by default.
 - The Opera Phishing filter is dubbed Opera Fraud Protection and is included in version 9.5+.
3. **Website forgery:** In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands. As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily. Another technique used is known as “cloaked” URL – domain forwarding and/or inserting control characters into the URL while concealing the weblink address of the real website.
4. **Flash Phishing:** Anti-Phishing toolbars are installed/enabled (see Table 5.2) to help checking the webpage content for signs of Phishing, but have limitations that they do not analyze flash objects at all. Phishers use it to emulate the legitimate website. Netizens believe that the website is “clean” and is a real website because anti-Phishing toolbar is unable to detect it.
5. **Social Phishing:** Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.
 - Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
 - The victim calls the bank on the phone numbers displayed in the mail.
 - The phone number provided in the mail is a false number and the victim gets redirected to the phisher.
 - Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank. For example, “Sir, we need to make sure that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity?”
 - Phisher gets the required details swimmingly.
6. **Phone Phishing:** We have explained “Mishing” – mobile Phishing attacks (“Vishing” and “Smishing”) in Chapter 3. Besides such attacks, phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords. See Box 5.7 to understand the innovative Phishing attack launched on “Android Market” website.

Box 5.6 Homograph Attack

The meaning of homograph is that two words are spelled the same way but differ in meaning (e.g., fair). Phishers use homograph attack on the Internationalized Domain Name (IDN) to deceive the netizens by redirecting them on the phony website which look like the original website.

ASCII has several characters and/or pairs of characters which look alike, for example, "0" (zero) and "O" (o alphabet in uppercase), "1" (L alphabet in lowercase) and "I" (i alphabet in uppercase). For example, the original website www.GOOGLE.com can be registered as www.G00GLE.com. Another example could be www.microsoft.com could be juggled as www.rnicrosoft.com (the letter "m" has been replaced with "r" and "n"). This phenomenon opens a rich vein of opportunities for Phishing attacks. The phisher could create and register a domain name which appears almost identical to an existing domain and takes the netizen to the phony website. Phisher could send E-Mail messages displaying the URL of a phony website, purporting to come from the original site, but directing netizens to the phony website. The phisher could easily record information such as passwords or account details through this spoofed website, while passing traffic through the original website. The netizens will never be able to notice the difference, until some suspicious or unusual activity occurs with their accounts. Visit <http://www.xn--goole-tmc.com/> to experience the explained phenomenon.

Source: http://en.wikipedia.org/wiki/IDN_homograph_attack (25 October 2010).

Box 5.7 Phishing Attack Launched through Android Market

Android: It is an open-source operating system (OS) for mobile phones and is based on Linux kernel. This OS has recently gained popularity with the release of Google's Nexus One phone. The Android Market is similar to iPhone App Store. Currently, around 22,000 applications are available on the Android Market.

According to an article available on <http://news.softpedia.com>, a malware writer succeeded to list a rogue Phishing application called 09Droid on the Android Market website. The application posed to be a shell for mobile banking applications, but, instead found, it is being used to obtain (steal) online banking credentials.

Travis Credit Union (TCU) issued an alert immediately, during the first week of December 2009, stating "Your mobile device may be at risk if you downloaded an application provided by 09Droid from the Android Marketplace; applications from 09Droid are NOT an authorized or legitimate downloadable application for TCU Mobile Banking." TCU also notified its customers through its website, Facebook page and E-Mail, although its services were not targeted by the rogue application.

First Tech Credit Union also issued a similar warning, stating "*The financial institution recommends that affected users take their phone to their mobile operator in order to make sure all traces of the malware are removed. The application attempts to steal financial information from consumers, for the likely purpose of Identity Theft.*"

Source: <http://news.softpedia.com/news/Phishing-Attack-Launched-from-Android-Market-131793.shtml> (26 July 2010).

Phishers usually take a broad approach by sending millions of E-Mail messages that appear to come from popular banks, online auction houses and other business houses. These E-Mail messages, pop-up windows and the websites appear to be official so that they can deceive many netizens to believe that they are legitimate. Unsuspecting netizens often respond to these requests for credit card numbers, passwords, account information or other personal and financial data. According to the 2009 Consumer Reports State of the Net Survey,^[18] Phishing scams cost US\$ 483 million in the US. Thus, we see that Phishing scams involve fraudulent E-Mail messages or fake websites designed to steal identity. Scam artists "phish" in an attempt to persuade millions of netizens/Internet users to disclose sensitive information. Now there is a new version of

an old scam called “Spear Phishing,” a targeted E-Mail attack that a scammer sends only to people within a small group, which is explained in the next section.

5.2.3 Spear Phishing

“Spear Phishing” is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here is how Spear Phishing scams work; Spear Phishing describes any highly targeted Phishing attack. Spear phishers send E-Mail that appears genuine to all the employees or members within a certain company, government agency, organization or group. The message might look like as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company (such as the person who manages the computer systems); it could include requests for usernames or passwords. Unfortunately, through the modus operandi of the Spear phishers, the E-Mail sender information has been faked or “spoofed.” While traditional Phishing scams are designed to steal information from individuals, Spear Phishing scams work to gain access to a company’s entire computer system. If you respond with a username or password, or if you click on the links or open the attachments in a Spear Phishing E-Mail, pop-up window or website, then you might become a victim of ID theft and you might put your employer or group at risk.

Spear Phishing also describes scams that target people who use a certain product or website. Scam artists use any information they can to personalize a Phishing scam to as specific a group as possible. Thus, “Spear Phishing” is a targeted E-Mail attack that a scammer sends only to people within a small group, such as a company. The E-Mail message might appear to be genuine, but if you respond to it, you might put yourself and your employer at risk. You can help avoid Spear Phishing scams by using some of the same techniques you have already used to help avoid standard Phishing scams (see Box 5.8).

Whaling

This is a specific form of “Phishing” and/or “Spear Phishing” – targeting executives from the top management in the organizations, usually from private companies. The objective is to swindle the executives into revealing confidential information. Whaling targets C-level executives sometimes with the help of information gleaned through Spear Phishing, aimed at installing malware for keylogging or other backdoor access mechanisms.



The names given to various *Internet scams* are found to be amusing. *Whaling* may have been derived from the fact that the people targeted are *top-ranking executives*. The difference between Spear Phishing and whaling appears to be a bit cloudy. It seems, whaling involves more extensive reconnaissance about the target rather than the target being enticed to be a victim of Spear Phishing attack.

E-Mails sent in the whaling scams are designed to masquerade as a critical business E-Mail sent from a legitimate business body and/or business authority. The content of an E-Mail usually involves some kind of falsified industry-wide concern and is meant to be tailored for executives.

Whaling phishers have also forged official looking FBI subpoena E-Mails and claimed that the manager needs to click a link and install special software to view the subpoena. In the case of the recent 2008 FBI subpoena whaling scam, 20,000 corporate CEOs were attacked. Approximately 2,000 of them fell for it and clicked on the whaling link, believing it would download a “special” browser add-on to view the entire subpoena document. In truth, the linked software was a keylogger that secretly recorded the CEOs passwords

and forwarded those passwords to the phisher men. As a result, each of the 2,000 compromised companies were further hacked in some way; a few of them were particularly damaged by the attacks.^[19]

Although the countermeasures of Phishing are covered at the end of Phishing section, however, see Box 5.8 to understand the countermeasures for Spear Phishing.

5.2.4 Types of Phishing Scams

We have seen how phishers use numerous methods and techniques to launch Phishing attacks. The prevalent types of Phishing^[20] scams are discussed in this section.

1. **Deceptive Phishing:** Phishing scams started by broadcasting deceptive E-Mail messages with the objective of ID theft. E-Mails are broadcasted to a wide group of netizens asking about the need to verify banking account information/system failure requiring users to re-enter their personal information/fictitious account charges and/or undesirable account changes/new free services requiring quick action. The netizens easily get enticed and reveal their information by responding to these E-Mails and/or clicking on weblinks or signing onto a fake website designed by the phisher.
2. **Malware-based Phishing:** It refers to scams that involve running Malicious Code on the netizens system. Malware can be launched as an E-Mail attachment or as a downloadable file from a website or by exploiting known security vulnerabilities. For example, small and medium businesses are always found to be ignorant to keep their operating systems (OS) antivirus software up to date with latest patch updates released by vendors. (See Section “The Bane of Malware” under Section 9.3, Chapter 9)
3. **Keyloggers:** We have explained keyloggers in Chapter 4. Malware can embed a keylogger to track keyboard input and send relevant information, maybe the keylogger log, to the phisher through the Internet. The keyloggers can also be embedded into netizen’s browser as a small utility program which can start automatically when the browser is opened or can be embedded into system files as device drivers.
4. **Session hijacking:** It is an attack in which netizens’ activities are monitored until they establish their bona fide credentials by signing into their account or begin the transaction and at that point the Malicious Code takes over and comport unauthorized actions such as transferring funds without netizen’s knowledge. See Box 5.9 to know more about “advanced form of Phishing.”
5. **In-session Phishing:** It is a Phishing attack based upon one web browsing session being able to detect the presence of another session (such as visit to an online banking website) on the same web browser and then a pop-up window is launched that pretends to be opened from the targeted session.

Box 5.8 Avoiding Spear Phishing Scams

There are few precautions you can take to avoid making yourself a victim of Phishing scam:

1. Never reveal personal or financial information in a response to an E-Mail request, no matter who appears to have sent it.
2. If you receive an E-Mail message that appears suspicious, call the person or organization listed in the *From* line before you respond or open any attached files.
3. Never click links in an E-Mail message that requests personal or financial information. Enter the web address into your browser window instead.
4. Report any E-Mail that you suspect might be a Spear Phishing campaign within your company.
5. You can use the Phishing filter – it scans and helps identify suspicious websites, and provides up-to-the-hour updates and reports about known Phishing sites (see Table 5.2 and Box 5.13, Chapter 5).

Box 5.9 Advanced Form of Phishing – Tabnapping or Tabjacking

Tabs are the web browser tabs and browser tabs that are not in use are called as *napping*. Most often, netizens work with multiple tabs open with different Web-browsing sessions on each one. In fact, netizens go hours without even realizing that, they have multiple tabs open.

When a netizen visits legitimate website such as banking website and opens a genuine webpage and that webpage is not used, that is, it is kept idle for some time because maybe netizen starts surfing other website (i.e., Googling) then, and when the netizen returns back to banking webpage, he/she gets redirected to phished webpage and he/she does not notice it, as he/she never closed the tab.

Phishers have identified a way to invade the browser tabs and change (i.e., replace) it to a page designed to steal the personal information. This is done by checking whether the webpage is idle for a particular time-period, and then phisher redirects the victim to a phished webpage. Phisher judge the idle webpages based on mouse movement, scroll bar movement and keystrokes.

Websites from banking/financial institutes as well as popular sites like Gmail, Orkut, Facebook and Yahoo are primary targets.

For example, netizen opens a tab to view the bank account. Netizen login on the website with his/her user ID and password and then go to another tab. While working with the other tab, phisher replaces the legitimate bank site webpage with a cloned login page developed to steal personal information. When he/she goes back to the tab, bank website, netizen assumes the webpage has timed out and hence requesting you to re-enter your password. If you do then you give the hacker access to your account.

Netizen believes this pop-up window is being a part of the targeted session and is used to steal netizen's personal information/data in the same way as with other Phishing attacks. The advantage of in-session Phishing attack is the phisher does not need the targeted website to be compromised but to rely on modern web browsers to support more than one session. To know more about this, visit http://en.wikipedia.org/wiki/In-session_Phishing (8 June 2010).

6. **Web Trojans:** It pops up to collect netizen's credentials and transmit them to the phisher while netizens are attempting to log in. Such pop-ups are usually invisible.
7. **Pharming:** It is a new threat evolved with a goal to steal online identity of the netizens and Pharming is known as one of the "P" in cybercrime (see Box 5.10).

In Pharming, following two techniques are used:

- **Hosts file poisoning:** The most popular operating system (OS) in the world is *Windows* and it has "host names" in their "hosts" file. A simple text file was used in web address (i.e., URL of website) during early days of the Internet [(i.e., before undertaking a DNS (Domain Name Server) lookup)]. Phisher used to "poison" the host file to redirect the netizen to a fake/bogus website, designed and developed by the phisher, which will "look alike" the original website, to steal the netizen's personal information easily.
 - **DNS-based Phishing:** Phisher tampers with a DNS so that requests for URLs or name service return a fake address and subsequently netizens are directed to a fake site. Netizens usually are unaware that they are entering their personal confidential information in a website controlled by phishers and probably not even in the same country as the legitimate website. DNS-based Phishing is also known as DNS hijacking. Along with this attack Click Fraud is an advanced form of technique evolved to conduct Phishing scams (see Box 5.11).
8. **System reconfiguration attacks:** Phisher can intrude into the netizens' system (i.e., computer) to modify the settings for malicious purposes. For example, URLs saved under *favorites* in the browser might be modified to redirect the netizen to a fake/bogus "look alike" websites (i.e., URL for a website of a bank can be changed from "www.xyzbank.com" to www.xyzbang.com.).

Box 5.10 Three Ps of Cybercrime – Phishing, Pharming and Phoraging

1. **Pharming:** It is an attack aiming to redirect a website's traffic to another bogus website. The term Pharming is a neologism based on "farming" and "Phishing."^[21] Pharming has become a major concern for businesses hosting E-Commerce and online banking websites. In Pharming, an attacker cracks vulnerability in an Internet service provider's (ISP) DNS server and hijacks the domain name of a commercial site. Therefore, anyone going to the legitimate site is then redirected to an identical but bogus site.
Antivirus softwares and Spyware removal softwares cannot protect against Pharming. The most efficient way to prevent Pharming is to ensure using secure web connections like HTTPS to access websites such as banking or financial institutions and at the same time accept the valid public-key certificates issued by trusted sources. A certificate from an unknown organization or an expired certificate should not be accepted.
2. **Phoraging (pronounced foraging):** It is defined as a process of collecting data from many different online sources to build up the identity of someone with the ultimate aim of committing identity theft.^[22]

Phoraging is information diving – searching for information with the aim of identity theft whereby a phisher collects data from various sources such as social networking sites, viruses and Spyware to build up the identity of a person.

The phishers always work in a smarter way, hence nowadays they are focusing on "matrimonial sites" as well as "social networking sites for professionals" (e.g., www.linkedin.com) to reveal personal information such as date of birth, personal E-Mail address, contact details and what not as the members (i.e., users of these websites) cannot post false information on these websites!!

Box 5.11 DNS Hijacking and Click Fraud

DNS hijacking: It is also known as *DNS redirection* and it is the practice of redirecting the resolution of Domain Name Server (DNS) names to rogue DNS servers, particularly for the practice of Phishing or to direct users' HTTP traffic to the ISP's own web servers where advertisements are served.^[23]

An illegal change to a DNS server directs URL to a different website. In some cases, the new website's URL may have one different letter in the name that might go unnoticed. The bogus website might offer similar and/or competing products for sale, or it may be a vehicle to publicly smear the reputation of the intended website.^[24]

DNS is used to interpret domain names such as www.<domainname>.com (e.g., www.yahoo.com) into an IP address. The IP address consists of numbers such as XXX.XX.XXX.X (e.g., 107.60.132.4) that give the domain a unique identification. An IP address is one-of-a-kind and unique, therefore, it can be used to trace Internet activity back to the PC user as well as identify the exact location of a website. Domain names are used to identify websites because they are easier to remember than a series of numbers that make up an IP address.

DNS hijacking is used by attackers with malicious intent who redirect or "hijack" the DNS addresses to bogus DNS servers for the purpose of injecting malware into your PC, promoting Phishing scams, advertising on high-traffic websites and any other related form of criminal activity.

Once the DNS address is hijacked to a bogus DNS server, it translates the legitimate IP address or DNS name into the IP addresses of malicious websites. DNS hijacking can occur with any website large or small and turn those websites into malicious websites without the knowledge of the netizens.

As the website owners depend upon legitimate DNS servers issued by their ISP, DNS hijackers use malware in the form of a Trojan to exchange the legitimate DNS server assignment by the ISP with a manual DNS server assignment from a bogus DNS server.

When netizens visit the reputable websites with legitimate domain names, they are automatically hijacked to a malicious website that is disguised as the legitimate one. The switch from the legitimate DNS server to the bogus DNS server goes unnoticed by both the netizen and the legitimate website owner. This opens up the malicious website to perform any criminal act that the phisher wishes because the netizen thinks that he/she is on the real website.

Box 5.11 DNS Hijacking . . . (Continued)

DNS hijacking also promotes Click Fraud with such programs as Google Adsense. As there are numerous DNS servers that are bogus, they form a network of websites which results in a lot of traffic. When there is a lot of traffic then you will find a lot of people clicking which results in Click Fraud. The attackers can rack up a lot of money with "click throughs" from programs such as Google Adsense who pay a commission for each click.

Click Fraud: It is a type of Internet crime that occurs in pay-per-click online advertising when a person automated script or computer program imitates a legitimate user of a web browser clicking on an advertisement (ad) for the purpose of generating a charge per click without having actual interest in the target of the ad's link. Click Fraud is the subject of some controversy and increasing litigation because of the advertising networks being a key beneficiary of the fraud.^[25]

It is an illegal practice that occurs when individuals click on a website click through advertisements (either banner ads or paid text links) to increase the payable number of click throughs to the advertiser. The illegal clicks could be either performed by having a person manually clicking the advertising hyperlinks or by using automated software or online Bots (see Section 2.6, Chapter 2) that are programmed to click these banner ads and pay per click text ad links. Research has indicated that Click Fraud is perpetrated by individuals who use Click Fraud to increase their own personal banner ad revenues and also by companies who use Click Fraud as a way to deplete a competitor's advertising budget.^[26] Visit the weblinks mentioned below to explore more on Click Fraud:

1. Exposing Click Fraud: http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078.html (18 June 2010).
2. The dark side of online advertising: http://www.businessweek.com/magazine/content/06_40/b4003001.htm (18 June 2010).

Click forensics is the industry leader in scoring, auditing and improving traffic quality for the online advertising community. For online advertisers, traffic quality management aims to improve campaign performance. The goal is to exclude low-quality traffic, eliminate Click Fraud and improve conversion rates. Click forensics optimizes online advertising campaigns. For online publishers, traffic quality management will attract and retain advertisers and ad networks to increase spend and earnings of ad per click. Click forensics has partnered with Yahoo! Click forensics is the leader in eliminating Click Fraud and is the publisher of the Click Fraud Index and the founder of the Click Quality Council. To know more about click forensics, visit <http://www.clickforensics.com/>

9. **Data theft:** Critical and confidential data getting stolen is one of the biggest concerns in the modern times. As more and more information resides on the corporate servers and the Web (including what happens with "cloud computing"), attackers have a boom time because taking away/copying information in electronic form is so easy! Unsecured systems (e.g., computers enabled with the Internet facility and with inappropriate security settings) are often found to be inappropriately maintained from cybersecurity perspective. When such systems are connected, the web servers can launch an attack with numerous methods and techniques. Data theft is a widely used approach to business espionage. Phishers can easily make profit from selling the stealth confidential communications, design documents, legal opinions and employee-related records to those who may want to embarrass or cause economic damage to competitors.
10. **Content-injection Phishing:** In this type of scam, phisher replaces part of the content of a legitimate website with false content to mislead the netizen to reveal the confidential personal information. For example, Phisher may insert Malicious Code to capture netizen's credentials that can secretly collect information and send it to phisher.
11. **Man-in-the-middle Phishing:** In this type of attack, phisher positions himself between the netizen and the legitimate website or system. Phisher records the input being provided by the netizen

but continues to pass it on to the web server so that netizens' transactions are not affected. Later on phisher can either sell or use the information or credentials collected when the user is not active on the system. This attack is very difficult to detect compared to other forms of Phishing. In Chapter 11, the man-in-the-middle (MITM) attack is discussed and explained in detail.

12. **Search engine Phishing:** It occurs when phishers create websites with attractive sounding offers (often found too good to be true) and have them indexed legitimately with search engines. Netizens find websites during their normal course of search for products or services and are trapped to reveal their personal information. For example, phishers set up fake/bogus banking websites displaying an offer of lower credit costs or better interest rates than other banks. Netizens who use these websites to save or make more from interest charges are encouraged to transfer existing accounts and enticed to giving up their details. See Box 5.12 to know more about search engine optimization (SEO) attack, which is an advance form of technique used by the attackers nowadays.
13. **SSL certificate Phishing:** It is an advanced type of scam. Phishers target web servers with SSL certificates to create a duplicitous website with fraudulent webpages displaying familiar "lock" icon. It is important to note that, in such types of scams, SSL certificates are always found to be legitimate as they match the URL of the fake pages that are mimicking the target brands but in reality had no connection to these brands displayed. It is difficult to recognize such websites; however, smart netizens can detect such deception after reviewing the certificate and/or whether the website has been secured with an extended validation SSL certificate.^[27]

Box 5.12 SEO Attacks – Beware While Searching through Search Engines!

Search engine optimization (SEO) is the practice of maximizing the volume or quality of traffic to a website (such as a blog) from search engines via natural or unpaid search results as opposed to other forms of search engine marketing (SEM) which may deal with paid inclusion. SEO considers how search engines work and what people search for. Optimizing a website primarily involves editing its content and HTML and associated coding to increase both its relevance to specific keywords and to remove barriers to the indexing activities of search engines.^[28]

Black hat SEO or spammeddexing is a technique^[30] which uses methods such as link farms, keyword stuffing and article spinning that degrade both the relevance of search results and the user experience of search engines. Search engines look for sites that employ these techniques to remove them from their indices.

According to security researcher Dancho Danchev, SEO attack abuses a common practice among websites – caching search queries – an activity designed to boost their rankings among major search engines, such as Google. Attackers inject common search terms and an iframe (<iframe> – HTML tag defines an inline frame that contains another document) script designed to send victims to other sites hosting Malicious Code. The search term and iframe redirect get cached in search engines such as Google.^[29]

The business of using SEO techniques to infuse legitimate websites has become a huge money spinner for attackers. The attackers take advantage of hottest news/stories on the Internet to spread malware – many of them profiting from high-profile deaths and disasters; for example, the death of celebrities such as Michael Jackson have provided rich attractive content for attackers trying to take advantage of trending news stories.

Techniques used for Black hat SEO attacks

1. **Fake antivirus:** Fake security alerts are flooded to netizens to entice them into executing the Malicious Code such as Activex Controls and/or paying for a bogus security product to install them.
2. **SEO page:** Pages stuffed with erroneous keywords, usually designed to feature highly in search engine results, are attacked to misdirect netizens to rogue websites. It is also known as SEO-poisoned pages.

Box 5.12 SEO Attacks – Beware While . . . (Continued)

3. **SEO poisoning:** It is a process of enticing search engine into ranking an SEO page high up in the search results and these results may be manipulated results known as “poisoned.”
4. **Black hat SEO kits:** These tools are used to launch and manage SEO attack. They are also known as search engine crawlers that poison search results to redirect netizens to rogue (i.e., bogus) websites. (Readers may visit <http://www.blackhatseo.com> to know more about this tool).

Distributed Phishing Attack (DPA)

We learned that the most common Phishing attack is launched using an E-Mail and fraudulent webpage/website to web host structure. Phisher sends lure E-Mails that entice the victim to follow the URLs displayed in the E-Mail which directs him/her to the phisher's website. As the victim is unable to verify/check legitimacy of the webpage/website, he/she submits personal information. Most often, the Phishing messages and webpages/websites masquerade as banks/financial institutions, government agencies or some other trustworthy entity that could probably ask for personal information.

Distributed Phishing attack is an advanced form of Phishing attack that works as per victim's personalization of the location of sites collecting credentials and a covert transmission of credentials to a hidden coordination center run by the phisher.

In this attack a large number of fraudulent web hosts (i.e., servers controlled by the phisher) are used for each set of lured E-Mails. Each server collects only a tiny percentage of the victim's personal information. This minimizes the possibility that the phisher shutdown the fraudulent web host within hours of initial mailing due to risk of detection of the origin of the fraudulent E-Mail. Each victim is referred to a unique webpage and in the extreme case the benefits of detection are kept minimum. Even if the victim recognizes the fraudulent E-Mail as a component of a Phishing attack, disabling the web server and/or the weblink to the fraudulent web server will not prevent any other potential victims from being betrayed of their personal information. Phishers launch attacks through thousands of servers using collections of compromised systems such as Botnets and/or zombies (explained in Chapters 1 and 2).



Visit the weblink mentioned below to know more examples of Phishing attacks launched through fake/bogus E-Mails: <http://www.doshelp.com/scams-fraud/index.html>

5.2.5 Phishing Toolkits and Spy Phishing

A Phishing toolkit is a set of scripts/programs that allows a phisher to automatically set up Phishing websites that spoof the legitimate websites of different brands including the graphics (i.e., images and logos) displayed on these websites. Phishing toolkits are developed by groups or individuals and are sold in the underground economy. These sophisticated kits are typically difficult to obtain, are quite expensive, and are more likely to be purchased and used by well-organized groups of phishers, rather than average users.

Phishers use hypertext preprocessor (PHP) to develop the Phishing kits. PHP is a general purpose scripting language that was originally designed for web development of dynamic webpages. PHP code is embedded into the HTML source script and interpreted by a web server with the help of a PHP processor module.

Most of the Phishing kits are advertised and distributed at no charge and usually these *free Phishing kits* – also called DIY (Do It Yourself) Phishing kits – may hide backdoors through which the phished information is sent to recipients (may be to the authors of Phishing kits) other than the intended users.

Following are few examples of such toolkits:

- Rock Phish:** It is a Phishing toolkit popular in the hacking community since 2005. It allows non-techies to launch Phishing attacks. The kit allows a single website with multiple DNS names to host a variety of phished webpages, covering numerous organizations and institutes.
- Xrenoder Trojan Spyware:** It resets the homepage and/or the search settings to point to other websites usually for commercial purposes or porn traffic.^[31]
- Cpanel Google:** It is a Trojan Spyware that modifies the DNS entry in the host's file to point to its own website. If Google gets redirected to its website, a netizen may end up having a version of a website prepared by the phisher.^[31]



DIY (Do It Yourself) Phishing kits that are available and/or distributed free of cost, aim not only just to steal personal information but also to infect the system with malware by embedding client-side vulnerabilities.

5.2.6 Phishing Countermeasures

The countermeasures explained in Table 5.1 will prevent malicious attacks that phisher may target to gain the unauthorized access to the system to steal the relevant personal information about the victim, from the system. It is always challenging to recognize/judge the legitimacy of a website while Googling (i.e., surfing on the Internet) and find it more intriguing while downloading any attachment from that particular website (see KRESV test in Appendix C in CD). Box 5.13 explains about “How to recognize legitimate websites,” while surfing on the Internet.

Table 5.1 | How to avoid being victim of Phishing attack

Sr. No.	Security Measures	Brief Description
1	Keep antivirus up to date	Important aspect is to keep antivirus software up to date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising the web address bar or mimicking the secure link (i.e., HTTPS)
2	Do not click on hyperlinks in E-Mails	It should always be practiced that, in case an E-Mail has been received from unknown source, clicking on any hyperlinks displayed in an E-Mail should be avoided. This may lead to either the link taking the victim to the website created by the phisher or triggering a Malicious Code installation on the system. Instead, to check out the link, manually retying it into a web browser is highly recommended.
3	Take advantage of anti-Spam software	Anti-Spam software can help keep Phishing attacks at a minimum. A lot of attacks come in the form of Spam and by using anti-Spam software, many types of Phishing attacks are reduced because the messages will never end up in the mailboxes of end-users.

(Continued)

Table 5.1 | (Continued)

<i>Sr. No.</i>	<i>Security Measures</i>	<i>Brief Description</i>
4	Verify https (SSL)	Ensure the address bar displays “https://” rather than just “http://” along with a secure lock icon than has been displayed at the bottom right-hand corner of the web browser while passing any sensitive information such as credit cards or bank information. One may like to check by double-clicking the lock to guarantee the third-party SSL certificate that provides the https service. Always ensure that the webpage is truly encrypted.
5	Use anti-Spyware software	Keep Spyware down to a minimum by installing an active Spyware solution such as Microsoft anti-Spyware and also scanning with a passive solution such as Spybot. If for some reason your browser is hijacked, anti-Spyware software can often detect the problem and provide a fix.
6	Get educated	Always update the knowledge to know new tools and techniques used by phishers to entice the netizens and to understand how to prevent these types of attacks. Report any suspicious activity observed to nearest cybersecurity cell.
7	Use the Microsoft Baseline Security Analyzer (MBSA)	The netizens on the Microsoft platform should use MBSA to ensure the system is up to date by applying all the security patches. MBSA is a free tool available on Microsoft’s website. This protects the IT systems against known exploits in Internet Explorer and Outlook (and Outlook Express) that can be used in Phishing attacks.
8	Firewall	Firewall can prevent Malicious Code from entering into the system and hijacking the browser. Hence, a desktop (software) such as Microsoft’s built-in software firewall in Windows-XP and/or network (hardware) firewall should be used. It should be up to date in case any cybersecurity patches have been released by the vendor.
9	Use backup system images	Always keep a backup copy or image of all systems to enable to revert to a original system state in case of any foul play.
10	Do not enter sensitive or financial information into pop-up windows	A common Phishing technique is to launch a bogus pop-up window when someone clicks on a link in a Phishing E-Mail message. This window may even be positioned directly over a legitimate window a netizen trusts. Even if the pop-up window looks official or claims to be secure, entering sensitive information should be avoided because there is no way to check the security certificate.
11	Secure the hosts file	The attacker can compromise the hosts file on desktop system and send a netizen to a fraudulent site. Configuring the host file to read-only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protects against tampering by outside attackers and keeps browsing safe.
12	Protect against DNS Pharming attacks	This is a new type of Phishing attack that does not Spam you with E-Mails but poisons your local DNS server to redirect your web requests to a different website that looks similar to a company website (e.g., eBay or PayPal). This is explained in Box 5.11.

Source: See [32] in References section.

Box 5.13 How to Judge/Recognize Legitimate Websites

1. ScanSafe (www.scansafe.com) was the first company in the world (founded in 2004) to offer web security. Scandoo (www.Scandoo.com) scans all search results to protect the user from visiting false websites (i.e., websites that spread malicious viruses or Spyware as well as protecting the user from viewing offensive content). Presently this site is not available as improvements for add-on features based on users' feedback is underway.
2. McAfee SiteAdvisor software (www.siteadvisor.com) is a free web security plug-in that provides the user with red, yellow and green website security ratings based on the search results. These ratings are based on tests conducted by McAfee after looking for all kinds of threats such as to name a few Phishing sites, E-Commerce vulnerabilities, browser exploits, etc.

Rating Icons

- McAfee SECURE:** Tested daily for hacker vulnerabilities.
- SAFE:** Very low or no risk issues.
- CAUTION:** Minor risk issues.
- WARNING:** Serious risk issues.
- UNKNOWN:** Not yet rated. Use caution.

Secure Search Icons

- SECURE SEARCH BOX:** Worry free searching.
- BROWSER BUTTON:** Validates site rating.

Source: <http://www.siteadvisor.com/howitworks/index.html>

In addition to the tools explained in Box 5.13, netizens may opt for anti-Phishing utilities (i.e., plug-ins) available for different browsers (Table 5.2) to be protected against Phishing attacks.

We learned that “E-Mail” is the popular medium used by phishers to entice the netizens; every netizen should imbibe it while responding to the received E-Mails. Hence, it is very important for the netizens who are not IT savvy (i.e., Techies – IT Professionals) but are Internet savvy (i.e., continuously surfing on the net) to discover the phished E-Mails. Figure 5.1 shows a simple flowchart explaining how to distinguish between a legitimate E-Mail and a phished E-Mail.

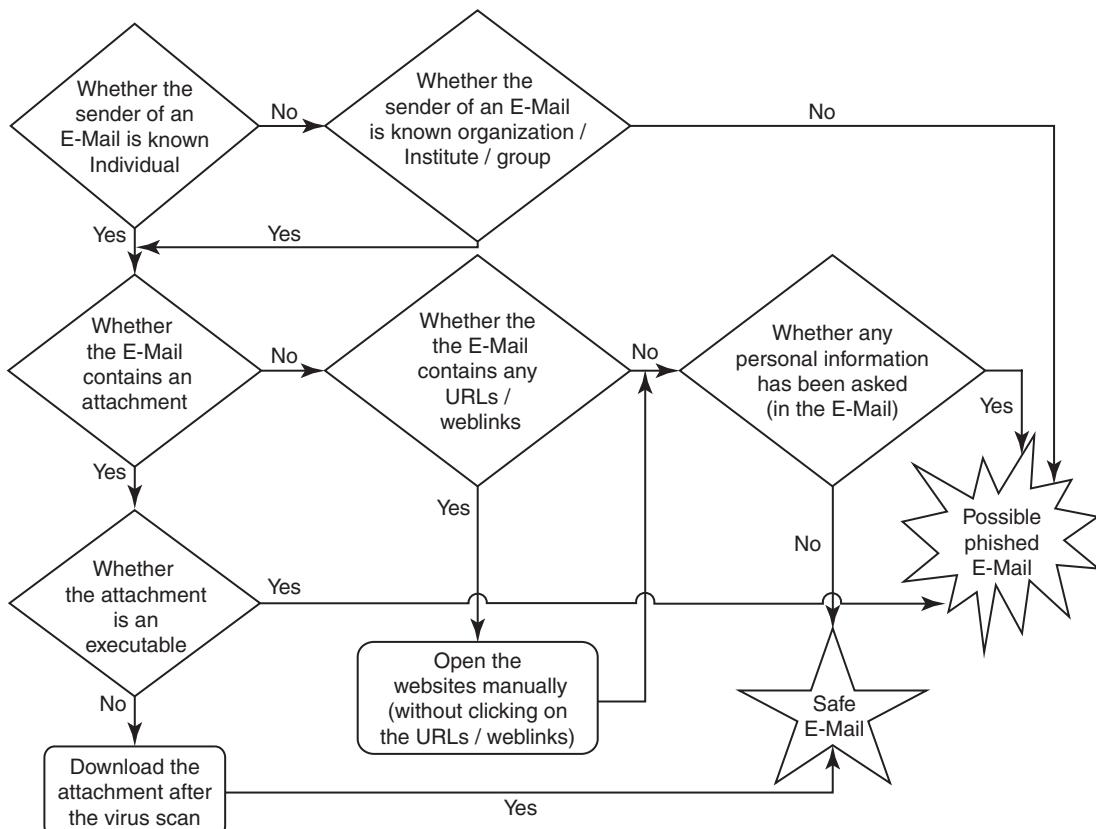
SPS Algorithm to Thwart Phishing Attacks

The proposal of system based on a simple filtering algorithm, Sanitizing Proxy System (SPS), has been suggested under the white paper by the authors Daisuke Miyamoto, Hiroaki Hazeyama and Youki Kadobayashi from Nara Institute of Science and Technology, Japan.

Table 5.2 | Anti-Phishing plug-ins

Sr. No.	Title	Website	Brief Description
1	Netcraft Toolbar	http://toolbar.netcraft.com/	It offers protection from Phishing attacks.
2	TrustWatch	http://wareseeker.com/free-trustwatch/	It has a toolbar for Internet Explorer users as well as has an extension for Firefox users.
3	ScamBlocker	http://www.earthlink.net/elink/issue95/security_archive.html	It is an Earthlink Toolbar feature that helps protect users from the latest Phishing threats.
4	PhishNet 1.2	http://download.cnet.com/PhishNet/3000-2144_4-10473931.html	It protects users from web Phishing scams.
5	SpoofStick	http://www.spoofstick.com/	It helps users detect spoofed (fake) websites.
6	Google safe browsing	http://www.google.com/tools/firefox/safebrowsing/	<ul style="list-style-type: none"> • It is used as an extension to Firefox. • It will alert when a webpage tries asking for user's personal or financial information. • It is available in Internet Explorer 7. • It helps protect users from entering Phishing sites.
7	Windows Internet Explorer's Phishing filter	https://phishingfilter.microsoft.com/PhishingFilterFAQ.aspx	

Source: See [33] in References section.

**Figure 5.1** | Phishing attack – flowchart.

The key idea behind SPS is that web Phishing attack can be immunized by removing part of the content that entices the netizens into entering their personal information. SPS sanitizes all HTTP responses from suspicious URLs with warning messages; however, netizens will realize that they are browsing Phishing sites. The white paper describes SPS filtering algorithm in simple 20 steps and dictates how it can be built in any proxy system, such as a server solution, a personal firewall or a browser plug-in.

The Phishing attack comprised two phases: (a) attraction and (b) acquisition. E-Mail Spoofing attracts netizens, as if it has been sent by a legitimate individual/organization. To acquire personal information, the spoofed E-Mail entices the netizens to execute the attached malware, such as a keylogger or a redirector, or to access a “spoofed” website.

The white paper summarizes the characteristics of SPS in the following points:

1. **Two-level filtering:** SPS employs two-level filtering composed of strict URL filtering and HTTP response sanitizing. By combining two filtering methods, netizens can be protected from revealing their personal information on Phishing sites.
2. **Flexibility of the rule set:** By filtering HTTP responses, the algorithm distinguishes between legitimate websites and other suspicious websites based on a rule set written by the operator of SPS.
3. **Simplicity of the filtering algorithm:** A simple two-level filtering algorithm can be described into 20 steps and can easily apply the SPS functions into existing proxy implementations, browser plugins or personal firewalls. SPS can be based on two different open-sourced proxy implementations to prove the simplicity and availability of the two-level filtering algorithm.
4. **Accountability of HTTP response sanitizing:** SPS prevents netizens from disclosing their personal information to Phishing sites by removing malicious HTTP headers or HTML tags from HTTP responses. SPS can also alert netizens about requested webpage containing suspicious parts that are under threat at the time of Phishing attacks.
5. **Robustness against both misbehavior of novice users and evasion techniques:** An SPS built-in proxy server can protect netizens from almost all deceit cases of web Spoofing, regardless of netizen's misbehavior and evasion techniques used by the phisher.

5.3 Identity Theft (ID Theft)

This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits (introduced in Section 1.5.21, Chapter 1). The person whose identity is used can suffer various consequences when he/she is held responsible for the perpetrator's actions. In many countries, specific laws make it a crime to use another person's identity for personal gain.^[34] As mentioned in the “introduction” section, ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).



Visit the weblink <http://njaes.rutgers.edu/money/identitytheft/default.asp> to undergo a quiz on identity theft to test your awareness and to get tips to avoid to be victim of identity theft.

The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as Identity Theft Resource Center (ITRC), with the objective to extend the support to the society to spread awareness about this fraud (see Box 5.14).

According to 2010 Report published by Javelin Strategy & Research^[35] the number of “identity fraud victims” were increased by 12% during 2009 and “amount of fraud” increased by 12.5%. Key statistics noted about total identity frauds in the US are as mentioned below:

1. The total fraud amount was US\$ 54 billion.
2. The average amount spent by the victim was US\$ 373 and the time of 21 hours to resolve the crime.
3. In total, 11.1 million adults were found to be victims of ID theft, which amounts to 4.8% of the population being a victim of identity fraud in 2009.
4. 13% of identity frauds were committed by someone who the victim knew.
5. Online methods accounted for only 11% of ID theft in 2009.
6. Offline methodology such as stolen wallets and paperwork account for almost half (43%) of all ID thefts.

Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below.^[36]

1. **Credit card fraud (26%):** The highest rated fraud that can occur is when someone acquires the victim’s credit card number and uses it to make a purchase. Chapter 11 (see Section 11.4.2) provides many illustrations on credit card frauds.
2. **Bank fraud (17%):** Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft. Chapter 11 (see Section 11.4.1) provides many illustrations on banking-related frauds.
3. **Employment fraud (12%):** In this fraud, the attacker borrows the victim’s valid SSN to obtain a job.
4. **Government fraud (9%):** This type of fraud includes SSN, driver license and income tax fraud.
5. **Loan fraud (5%):** It occurs when the attacker applies for a loan on the victim’s name and this can occur even if the SSN does not match the name exactly.

Readers may like to visit Section 11.7, Chapter 11, where many forms of online scams are described. It is important to note the various usage of ID theft information.^[37]

1. 66% of victims’ personal information is used to open a new credit account in their name.
2. 28% of victims’ personal information is used to purchase cell phone service.
3. 12% of victims end up having warrants issued in their name for financial crimes committed by the identity thief.

The statistics proves the importance of ID theft and the frauds related with ID theft are increasing day-by-day. ITRC, in the US, is putting enormous efforts to create awareness among the society to reduce such frauds (see Box 5.14).

Box 5.14 Identity Theft Resource Center (ITRC)

Identity Theft Resource Center (ITRC) is a non-profit, nationally respected organization situated at San Diego, CA, USA, dedicated exclusively to the prevention of identity theft. The ITRC provides support to the society for public education about identity theft. The organization also provides advice to governmental agencies, law enforcement agencies and business organizations about evolving and growing threat of identity theft.

Box 5.14 Identity Theft Resource . . . (Continued)

1. During December 1999, Linda and Jay Foley founded the ITRC, under the umbrella of Privacy Rights Clearinghouse, originally named Victims of Crimes Extended Services (VOICES).
2. In Spring 2000, the name of the organization was changed to the Identity Theft Research Center (ITRC) and was headed by Linda Foley.
3. During 2001, Jay Foley joined the ITRC as a full-time director.
4. In 2007, ITRC staff developed and published a completely new website www.idtheftcenter.org, which is a Google ranked 7 website.



Visit the weblink mentioned below to undergo the tests and quiz to know individuals preparedness toward identity theft: http://www.idtheftcenter.org/artman2/publish/c_theft_test/index.shtml

According to a September 2003 survey conducted by the FTC, an estimated 10 million people in the US found out that they were victims of ID theft in the previous year.^[38] In spite of enough awareness being created and/or trainings conducted in the society, people have their own beliefs about not being a victim of ID theft fraud. Table 5.3 explains myths and facts about ID theft.

Table 5.3 | Myths and facts about identity theft

<i>Sr. No.</i>	<i>Myth</i>	<i>Fact</i>
1	There's no way to protect yourself from identity theft.	The risk of identity theft can be minimized by taking preventive measures such as keeping financial records duly protected and private, shredding junk mail, and keeping an eye on who sees/overlooks your personal information.
2	Identity theft is only a financial crime.	Financial identity theft is theft of information for financial gain, which is most prevalent. However, other types of identity theft are equally dangerous. For example, medical identity theft of personal medical records is used to access medical treatment or drugs, or to make false insurance claims.
3	It's my bank's fault if I become a victim of identity theft.	Some identity crime does originate with the theft of bank records or is perpetuated by lax security practices. However, the majority of identity theft begins elsewhere. Personal information may be stolen with low-technology tools such as a lost or stolen wallet, checkbook, or a debit or credit card, or more high-technology methods, such as skimming, Phishing and hacking.
4	It is safe to give your personal information over the phone if your caller ID confirms that it is your bank.	It is never safe to give personal information to unsolicited callers, no matter who they say they are. Caller IDs are easily spoofed. If you believe the caller is legitimate, hang up and call the bank back at its listed phone number.
5	Checking your credit report periodically or using a credit monitoring service is all you need to do to protect yourself from identity theft.	If anyone wants to be vigilant about identity theft, one should check their credit report regularly and one should also review their bank and credit card statements regularly. One can obtain one's free credit report in the US from each of the three credit bureaus per year from www.AnnualCreditReport.com

(Continued)

Table 5.3 | (Continued)

<i>Sr. No.</i>	<i>Myth</i>	<i>Fact</i>
6	My personal contact information (mailing address, telephone number, E-Mail address, etc.) is not valuable to an identity thief.	Any information that could be used by a thief to impersonate you should be protected. For example, many people use their E-Mail address as a user ID for online accounts. Consider making your information available on a need-to-know basis only. Often, businesses ask for personal information they really don't need, and will simply omit information you're not willing to give.
7	Shredding my mail and other personal documents will keep me safe.	Shredding documents that contain personal information before you throw them away is a great way to protect yourself from "dumpster diving," which occurs when attackers search the trash for personal information. However, relying on your shredder alone to protect you is like locking one window while leaving the rest of your house wide open. Think defensively: secure your personal information in your home, in your car and at work, and always use safe online security practices.
8	I don't use the Internet so my personal information is not exposed online.	Your personal information appears in more places than you might realize, whether it's your medical records, a job application or a school emergency contact form. Many of these records are kept in electronic databases and transmitted online. Social networking sites are another good source of personal information for identity thieves. Even if you do not use them yourself, your friends or members of your family may be sharing personal information about you. Not using the Internet may offer some protection, but it won't keep you safe from online criminals.
9	Social networking is safe.	Social networking sites such as Facebook, MySpace and Twitter can be fun to use. However, they can be dangerous when it comes to your identity. These sites are used by attackers and others to steal information, trick people and promote a variety of scams. To protect yourself, avoid making personal information available to large groups of "friends," take advantage of the privacy controls offered by most of these sites, and use common sense.
10	It is not safe to shop or bank online.	Like social networking, shopping and banking online are safe as long as you use common sense and make good choices about where and how you do it. Most importantly, always take care to confirm that a site is legitimate before you use it, watch out for copycat sites and keep your computer safe from viruses.

Source: See [39] in References section.

5.3.1 Personally Identifiable Information (PII)

The fraudster always has an eye on the information which can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual. PII has four common variants based on personal, personally, identifiable and identifying.

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity:

1. Full name;
2. national identification number (e.g., SSN);
3. telephone number and mobile phone number;

4. driver's license number;
5. credit card numbers;
6. digital identity (e.g., E-Mail address, online account ID and password);
7. birth date/birth day;
8. birthplace;
9. face and fingerprints.

The fraudster may search for following about an individual, which is less often used to distinguish individual identity; however these can be categorized as potentially PII because they can be combined with other personal information to identify an individual.

1. First or last name;
2. age;
3. country, state or city of residence;
4. gender;
5. name of the school/college/workplace;
6. job position, grades and/or salary;
7. criminal record.

The information can be further classified as (a) non-classified and (b) classified. [Classification scheme is also explained in Chapter 9 (Section 9.11) in the context of media and asset protection.]

1. Non-classified information

- **Public information:** Information that is a matter of public record or knowledge.
- **Personal information:** Information belongs to a private individual but the individual commonly may share this information with others for personal or business reasons (e.g., addresses, telephone numbers and E-Mail addresses).
- **Routine business information:** Business information that do not require any special protection and may be routinely shared with anyone inside or outside of the business.
- **Private information:** Information that can be private if associated with an individual and individual can object in case of disclosure (e.g., SSN, credit card numbers and other financial information).
- **Confidential business information:** Information which, if disclosed, may harm the business (e.g., sales and marketing plans, new product plans and notes associated with patentable inventions).

2. Classified information

- **Confidential:** Information that requires protection and unauthorized disclosure could damage national security (e.g., information about strength of armed forces and technical information about weapons).
- **Secret:** Information that requires substantial protection and unauthorized disclosure could seriously damage national security (e.g., national security policy, military plans or intelligence operations).
- **Top secret:** Information that requires the highest degree of protection and unauthorized disclosure could severely damage national security (e.g., vital defense plans and cryptologic intelligence systems).

ID theft fraudsters and/or industrial/international spies target to gain the access to private, confidential, secret and top secret information.

5.3.2 Types of Identity Theft

Identity is stolen in order for someone to commit the crime. ID theft is related to many areas:

1. Financial identity theft;
2. criminal identity theft;
3. identity cloning;
4. business identity theft;
5. medical identity theft;
6. synthetic identity theft;
7. child identity theft.

Financial Identity Theft

Financial ID theft includes bank fraud, credit card fraud, tax refund fraud, mail fraud and several more. In total, 25 types of financial ID thefts are investigated by the US Secret Service. Financial identity occurs when a fraudster makes a use of someone else's identifying details, such as name, SSN and bank account details, to commit fraud that is detrimental to a victim's finances. For example, the fraudster fraudulently can open a new credit card account in the victim's name and the card charges up, payment is neglected, leaving the victim with bad credit history (i.e., horrible credit score) and a world of debt. In some cases, the fraudster will completely take over a victim's identity, which enables the fraudster to easily open bank accounts, multiple credit cards, purchase a vehicle, receive a home mortgage or even find employment in the victim's name.

The process of recovering from the crime is often expensive, time-consuming and psychologically painful. Many a times, before a crime is detected, the fraudster is capable of running up hundreds to thousands of dollars worth of debt in the victim's name. This type of fraud often destroys a victim's credit and it may take weeks, months or even years to repair. As technology moves along and fraudsters become more advanced, financial ID theft will continue to pose a great threat to many individuals.

Criminal Identity Theft

It involves taking over someone else's identity to commit a crime such as enter into a country, get special permits, hide one's own identity or commit acts of terrorism. These criminal activities can include:

1. Computer and cybercrimes;
2. organized crime;
3. drug trafficking;
4. alien smuggling;
5. money laundering.

Individuals who commit ID theft are not always out to steal the victim's money or ruin victim's credit. This type of fraud/theft occurs when a fraudster uses the victim's name upon an arrest or during a criminal investigation. The personal information given by a fraudster to a law enforcement officer may include counterfeited document such as driver's license, birth certificate, etc. Unfortunately, the victim of criminal ID theft may not know what warrant has been issued under his/her name for quite some time. The victim will only come to know in case of being detained on a routine traffic stop and arrested due to outstanding and overdue debts. In some cases, the fraudster will appear in court for the violation and enter a guilty plea without the victim's knowledge. This may place the victim's name into countywide or state-wide criminal database with a huge blemish language on the record.

There have been several instances where victims of criminal ID theft do not learn of an impersonation until being denied for employment or terminated from a job. This occurs when an employer conducts a criminal background search and finds that the victim has a criminal history that he/she lied about or charges that forbid him/her from working in that particular environment. When this happens, there is very little a victim can do to salvage the job, as an employer has the right to proceed with termination over entering false information on an application.

The victims of this crime are left with the burden to clear their own name in the eyes of the criminal justice system. It is very important to act quickly in order to minimize the damage and get your life back in order. What makes the process so difficult is the fact that officials working within the criminal justice system are the only ones capable of correcting the data. It is very crucial and important to contact local police department immediately in case of becoming a victim of criminal ID theft. This should be the first step in building a case and clearing your name.

Identity Cloning

Identity cloning may be the scariest variation of all ID theft. Instead of stealing the personal information for financial gain or committing crimes in the victim's name, identity clones compromise the victim's life by actually living and working as the victim. ID clones may even pay bills regularly, get engaged and married, and start a family. In summary, identity cloning is the act of a fraudster living a natural and usual life similar to a victim's life, may be at a different location.

An identity clone will obtain as much information about the victim as possible. They will look to find out what city and state the victim (he/she) was born in, what street he/she grew up on, where he/she attended school and what relationships he/she may have been involved in. They will also want to know information concerning the victim's parents and other family members. In a nutshell, identity clones want as much personal information about the victim as they can attain. This enables them to answer questions in an informative manner when they are on the move or asked about the victim's life.

Business Identity Theft

"Bust-out" is one of the schemes fraudsters use to steal business identity; it is paid less importance in comparison with individual's ID theft. A fraudster rents a space in the same building as victim's office. Then he applies for corporate credit cards using victim's firm name. The application passes a credit check because the company name and address match, but the cards are delivered to the fraudster's mailbox. He sells them on the street and vanishes before the victim discovers the firm's credit is wrecked.^[40] Hence, it is extremely important to protect business sensitive information (BSI) to avoid any further scams.

BSI is the information about the business/organization, privileged in nature and/or proprietary information which, if it is compromised through alteration, corruption, loss, misuse or unauthorized disclosure, could cause serious damage to the organization. Such information is like a "sensitive asset" for the organization.^[41]

Identity theft in the business context occurs most often when someone knocks off the victim's product and masquerades their shoddy goods as victim's. It is a kind of intellectual property theft. Nowadays, technology has made it easier for the trademarks and security devices such as holograms to be knocked off swimmingly. The consumers should no longer rely on trademarks alone to certify the authenticity of the goods and should verify their source of origin.



Visit the counterfeit gallery at the International Anti-Counterfeit Coalition website at <http://iacc.org/about-counterfeiting/counterfeit-gallery/index.php> to test your ability to spot fake consumer products.

Business ID theft may fuel economic and industrial espionage – which is most commonly associated with technology-heavy industries such as computer software and hardware, biotechnology, aerospace, telecommunications, transportation and engine technology, automobiles, machine tools, energy, materials and coatings and so on. See Box 5.15 to know more about industrial spy network.

The consequences of business ID theft may call for a disaster to the business, such as call out from market and damage to the reputation, and hence it is extremely important to employ countermeasures for such type of attacks (see Table 5.4).

Box 5.15 Chinese Ghost Net

China has been accused of attacking a number of groups and institutions through the use of cyber espionage, a fact which already put it high on the research team's "countries of interest" list. GhostNet is a spy network, accused to have been controlled from China, with the objective to hack into government and private sector companies in 103 countries.

GhostNet directs infected computers to download a Trojan known as "gh0st RAT" (also reported as Remote Access Tool) that allows attackers to gain complete and real-time control from commercial Internet access accounts located on the island of Hainan, People's Republic of China. The investigations reveal that GhostNet is capable of taking the entire control of infected computers, including searching and downloading specific files, and covertly operating attached devices such as microphones and web cameras.

This spying attack started with online espionage activities against the Tibetan community and subsequently targeted Foreign Ministries, embassies, banks and NEWS organizations across the world. Although Chinese Government has rejected all these allegations, it is reported that Foreign Ministries of Iran, Bangladesh, Latvia, Indonesia, the Philippines, Brunei, Barbados and Bhutan had been spied on remotely, and the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan were hacked.

The Toronto researchers listed the systems mentioned below as the ones they are highly confident to have been compromised:

1. Office of the Dalai Lama, India.
2. Tibetan Government in Exile, India.
3. Association of Southeast Asian Nations (ASEAN).
4. Asian Development Bank.
5. Associated Press, UK.
6. Consulate General of Malaysia, Hong Kong.
7. Department of Foreign Affairs, Indonesia.
8. Department of Foreign Affairs, Philippines.
9. International Campaign for Tibet.
10. NATO.
11. Russian Federal University Network, Russian Federation.
12. Students for a Free Tibet, US.
13. Taiwan Government Service Network, Taiwan.

If it assumed that GhostNet is a fluke and a deliberate creation of a foreign power (or the creation of a group) other than China, with the objective to search the information to sell at a profit, then there is the likelihood of many GhostNets in operation around the world, which may be operating with some specific objective. The story concludes as, GhostNet is neither the first nor the only one of its kind.

Source: <http://www.darkgovernment.com/news/chinas-ghostnet/>

Table 5.4 | Business identity theft – countermeasures

Sr. No.	Facet	Brief Description
1	Secure your business premises with locks and alarms	Alarm systems are effective deterrents to criminals thinking of breaking into your business, including that intent on identity theft – especially alarm systems that are monitored by a security company. Make sure that external doors have deadbolts and that exposed windows are secured with security film, bars, screens or shatter-proof glass.
2	Put your business records under lock and key	Store your physical business records, such as customer records and other data on paper, locked in filing cabinets – and lock the filing cabinets at night, or at those times during the day that you and your staff will not be “supervising” access (such as lunch time). Put copies of system and database backups and “important” business data in your safe (or in your security deposit box at the bank if you don’t have an onsite safe).
3	Shred, shred and shred	Business records of any kind should never just be tossed into the trash or recycling bin where they can become a bonanza for criminals wanting to commit on identity theft; instead, all business records that you no longer have a use for should be shredded. Businesses that operate out of small and home offices can buy inexpensive shredders at any office supply store; for businesses with volumes of material to be disposed of, there are shredding services that will come and do what needs to be done. Pay special attention to the mail, a favorite source for identity theft. Anything that has your name and address on it should be shredded, and that includes most bills.
4	Be cautious on the phone	It’s easy for someone to pretend to be someone they’re not on the phone. Whether it’s someone who wants personal information on a particular customer, or someone who claims they need to verify one of your personal accounts, don’t give out information over the phone unless you can positively confirm the caller’s identity. <i>“Information thieves and stalkers tell authorities over and over how easily they were able to obtain all sorts of valuable information simply by calling small business owners or personnel departments and asking. Posing as government agencies or credit grantors or health insurance providers, these thieves have found that a well-crafted, believable story can often get past the best locking file cabinets or password-protected computers,”</i> warns the Better Business Bureau.
5	Limit access to your IT systems	Your computer network needs to be password protected, of course, so that anyone who wanders through your office can’t just access your network. However, you also need to consider issues of internal network access. Does every employee needs to access programs or databases that may contain sensitive information? Password-protect these too and grant access on a “need-to-know” basis to help cut down identity theft.
6	Protect the IT systems from hackers	Hacking into company systems and databases appears to have become a favorite identity theft technique – perhaps because it’s very easy. Your computer network needs to be protected by firewalls, which help keep out intruders by shutting out unauthorized people and letting others go only to the areas they have privileges to use. You can purchase firewalls at any computer store (or online). Another option for small or home businesses is to purchase and install a small (four to eight port) router. These often have firewall protection capability. If you’re running Windows operating systems, it’s also important that you keep your operating system updated, installing the various patches as they come out. Often these patches are fixes for security holes. (If you use Windows XP, you will be alerted automatically to these updates.)

(Continued)

Table 5.4 | (Continued)

<i>Sr. No.</i>	<i>Facet</i>	<i>Brief Description</i>
7	Create the awareness that the Internet is a dangerous place	Ordering something off the Net using a credit card is not dangerous, as long as you are placing your order through a secure site. However, there are other dangers, such as Spyware and viruses, which attempt to download automatically when you or your employees visit certain sites. If you are using Internet Explorer, make sure that you go to “Internet Options” and set the security options to a higher setting on each computer; the default is set to allow just about anything to download. Moreover, if your company has a website, be careful as to what kind of information you post on your site and how. If you are going to place sensitive information on the Net (something you should be very cautious about), such as financial data or customer databases, it needs to be password-protected and encrypted.
8	Avoid broadcasting information	“The other day while making a purchase at a computer store, an associate asked me for my phone number and popped up all my personal information on a terminal in front of him – right in plain view of five other customers! I was so curious to ask him if he wanted to read it all out loudly to make it even easier for all of them to remember it.” This sort of cavalier sharing of personal information, which makes identity theft so easy, has to stop. Train your employees to be sensitive to customer information issues, making sure that they keep customer information private when they’re dealing with individual customers. Turning computer screens so that they can’t be viewed by anyone except the operator and other practices such as not repeating customer information loudly or not leaving files with customer information lying open on counters should be taken into consideration.
9	Create and enforce a organization-wide information security policy	The purpose of your security policy is to educate your employees about issues such as identity theft and data protection. It should include information on E-Mail policies (such as what E-Mail filters are in place and how to deal with suspicious E-Mail), computer network access, Internet use policies (such as how to increase browser security settings and safe practices, such as disconnecting from the Net after using it), customer information protection strategies and how to report incidents or violations. In other words, a manual of the issues involved with security and threats such as identity theft and what to do about them.
10	Disconnect the access of ex-employees immediately	When employees no longer work for your business, you need to be sure that their access to your computer network and company data is cut off immediately. Will all this create more trouble and expense for your small business? Yes. But unfortunately, with identity theft becoming rampant, taking these steps to prevent identity theft for you and your customers is necessary.

Source: See [42] in References section.

Medical Identity Theft

India is known to have become famous for “medical tourism.” Thousands of tourists, every year visit India with dual purpose – touring the country plus getting their medical problems attended to (surgeries, total health check, Kerala massage, etc.) because India has made name for good quality and yet reasonable priced (compared with Europe and the US) in medical services. In the process thousands of medical records of foreigners as well as locals who avail medical facility get created. This has created a boom for cybercriminals.

Healthcare facilities now are very different compared to how they were used a decade back. There are greater opportunities for protected health information (PHI) changing hands when multiple agencies are connected over computer networks and the Internet – for example, medical representatives, health officers, doctors, medical insurance organizations, hospitals, etc. to name a few (see Fig. 5.2).

Medical facility providers are moving from cumbersome paper records to faster and easier file and trace electronic records; however, the concern over medical ID theft^[43] is growing. The stolen information can be used by the fraudster or sold in the black market to people who “need” them. This could lead to many more cases. For example, invoice of thousands of dollars of emergency medical services was received by a man situated in Houston (Texas), who had never had any health issues, as reported in the New York Times. A fraudster had used this man’s identity for the fraudster’s emergency medical needs.

Medical ID theft can be dangerous not only from a financial perspective as explained in the case above, but also from a medical perspective. If the fraudster has successfully stolen the victim’s identity and received treatment, the record can become part of a victim’s permanent medical record. For example, a patient could be unconscious after an accident. The emergency room reads that during a previous admission the “patient” indicated he/she is not allergic to the medication the doctor believes will be most beneficial for the unconscious patient. Relying on the prior medical record, the doctor administers that drug which, in reality, the patient is severely allergic to.

According to a 2008 Identity Theft Resource Center survey, some of the reasons why medical ID theft is particularly damaging the victims include:

1. Approximately one-third of victims of medical ID theft surveyed had someone else’s medical information or medical history on their medical record, increasing the possibility of patients being treated incorrectly because of incorrect medical records.

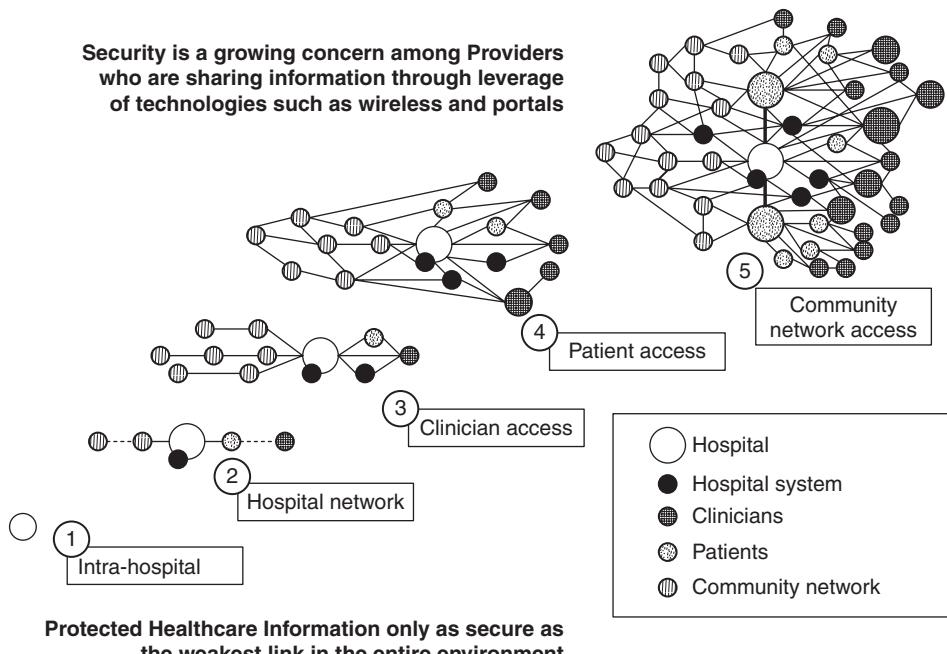


Figure 5.2 | Medical domain – interconnected entities.

2. More than 10% of victims of medical ID theft surveyed were denied health or life insurance for unexplained reasons.
3. More than two-third of victims surveyed receive a bill for medical services that were provided to an imposter.

ModernHealthcare.com reported a noticeable spike in attempted medical ID theft. This has been confirmed during June 2008 wherein the University of Utah Hospital announced that the personal information of 2.2 million patients had been stolen.

The World Privacy Forum estimates that there are more than 250,000 cases of medical ID theft each year and acknowledges that medical ID theft is a crime that can cause great harm to the victims. Medical ID theft has been addressed by HIPAA and HITECH Acts in the US (see Box 5.16 as well as Fig. 5.2).

Synthetic Identity Theft

This is an advanced form of ID theft in the ID theft world. The fraudster will take parts of personal information from many victims and combine them. The new identity is not any specific person, but all the victims can be affected when it is used.

Child Identity Theft

Parents might sometimes steal their children's identity to open credit card accounts, utility accounts, bank accounts and even to take out loans or secure leases because their own credit history is insufficient or too damaged to open such accounts.

Box 5.16 HIPAA, PHI and HITECH

The Health Insurance Portability and Accountability Act (HIPAA) enacted by the US Government in 1996, was sponsored by Senator Edward Kennedy and Senator Nancy Kassebaum. This act not only protects the Health Insurance Coverage but also detects the security and privacy of health data.

1. **HIPAA – Title I:** It regulates the availability and extent of group health plans and certain individual health insurance policies.
2. **HIPAA – Title II:** It defines numerous offenses relating to healthcare and sets civil and criminal penalties for them. It also creates several programs to control fraud and abuse within the healthcare system.

Protected Health Information (PHI) is any information held by the healthcare organizations (such as hospitals, nursing homes, medical service providers and medical insurance companies) which can be interpreted broadly and includes any part of an individual's medical record or payment history.

Health Information Technology for Economic and Clinical Health Act (HITECH Act) is enacted as part of the American Recovery and Reinvestment Act of 2009. Subtitle D of HITECH Act dictates the privacy and security concerns associated with the electronic transmission of health information and extends the complete Privacy and Security Provisions of HIPAA to business associates of healthcare organizations (see Box 6.18, Chapter 6).

Source: http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

5.3.3 Techniques of ID Theft

Identity theft can affect all aspects of a victim's daily life and often occurs far from its victims. The attackers use both traditional, that is human-based, methods as well as computer-based techniques.

1. **Human-based methods:** These methods are techniques used by an attacker without and/or minimal use of technology
 - *Direct access to information:* People who have earned a certain degree of trust (house cleaners, babysitters, nurses, friends or roommates) can obtain legitimate access to a business or to a residence to steal the required personal information.
 - *Dumpster diving:* Retrieving documents from trash bins is very common and explained in Chapter 2.
 - *Theft of a purse or wallet:* Wallet often contains bank credit cards, debit cards, driving license, medical insurance identity card and what not. Pickpockets work on the street as well as in public transport and exercise rooms to steal the wallets and in turn sell the personal information.
 - *Mail theft and rerouting:* It is easy to steal the postal mails from mailboxes, which has poor security mechanism and all the documents available to the fraudster are free of charge, for example, Bank Mail (credit cards and account statements), administrative forms or partially completed credit offers. The fraudster can use your name and other information that may prove to be harmful for an individual in the near future. Therefore, return items to the sender or request a change of address.
 - *Shoulder surfing:* People who loiter around in the public facilities such as in the cybercafes, near ATMs and telephone booths can keep an eye to grab the personal details. This is already explained in Chapter 2.
 - *False or disguised ATMs ("skimming"):* Just as it is possible to imitate a bank ATM, it is also possible to install miniaturized equipment on a valid ATM. This equipment (a copier) captures the card information, using which, duplicate card can be made and personal identification number (PIN) can be obtained by stealing the camera films.
 - *Dishonest or mistreated employees:* An employee or partner with access to the personal files, salary information, insurance files or bank information can gather all sorts of confidential information and can use it to provide sufficient damage.
 - *Telemarketing and fake telephone calls:* This is an effective method for collecting information from unsuspecting people. The caller who makes a "cold call" (supposedly from a bank) asks the victim to verify account information immediately on the phone, often without much explanation or verification. This attack is known as Vishing and it is explained in Chapter 3.
2. **Computer-based technique:** These techniques are attempts made by the attacker to exploit the vulnerabilities within existing processes and/or systems.
 - *Backup theft:* This is the most common method. In addition to stealing equipment from private buildings, attackers also strike public facilities such as transport areas, hotels and recreation centers. They carefully analyze stolen equipment or backups to recover the data.
 - *Hacking, unauthorized access to systems and database theft:* Besides stealing the equipment and/or hardware, criminals attempt to compromise information systems with various tools, techniques and methods (explained in Chapter 4) to gain unauthorized access (see Box 6.1, Chapter 6) to download the required information. See Box 5.17 to know advanced form of ID theft while the victim is in travel mode.
 - *Phishing:* Phishing is explained in Section 5.2.
 - *Pharming:* Pharming is explained in Box 5.10. In summary, the attackers setup typo or matching domain names of the target (usually of popular banks and financial institutions) and install websites with similar look and feel. Hence, even if the user types-in incorrect URL (e.g., instead of www.xyzbank.com, URL is punched as www.xyzbanc.com), the user gets the website with

Box 5.17 Geotagging

Geotagging is the process of adding geographical identification (such as latitude and longitude data) inside the metadata to various media such as photographs, video and/or SMS messages. Besides latitude and longitude coordinates, it can also include altitude, bearing, distance and place names. It is commonly used for photographs. Geotag information, embedded in the metadata, is stored into Exchangeable Image File (EXIF) format or into eXtensible Metadata Platform (XMP) format under the photographs stored in JPEG file format. These data are not visible in the picture itself but are read and written by special programs and most digital cameras and modern scanners. The EXIF data can be read by special programs (visit www.digital-photo-software-guide.com and www.photo-freeware.net for EXIF editors), which can provide maps of the location where the photo was taken. The same geotagged photos, when shared online, can also be linked to several map services.

Risks associated with Geotagging

1. The netizens snap photographs of their families/relatives/friends during a vacation, using cell phones/digital cameras and then immediately upload them on social networking websites such as Twitter/Facebook/Orkut/Myspace. The attacker can decipher these photographs (i.e., EXIF data) to know where the victim is located when he/she took the photographs.
2. The attacker can easily find when the family is not at home and the house is vulnerable to burglary attack.
3. A simple photograph of a car parked outside the house can provide the information about the address of the home.

How to protect from Geotagging

1. Turn OFF location information into cell phones/PDAs and cameras (visit <http://www.icanstalku.com/how.php> to know "How to disable this configuration").
2. Refer to the manual of the device and/or consult the manufacturer of the device to disable this intrusive feature.
3. Be skeptical about uploading the photographs on social networking websites.
4. Be careful while uploading/sharing photographs of kids and spouse through E-Mails and/or uploading those on social networking websites while they may have shared with you while traveling on their own.

Source: <http://en.wikipedia.org/wiki/Geotagging>

the same look and feel. This website is not real and is hosted with the sole purpose to extract personal information from the netizen.

- *Redirectors:* These are malicious programs that redirect users' network traffic to locations they did not intend to visit. For example, port redirection program is loaded by compromising the server and all HTTP Port 80 requests may be redirected to attacker. The highest volume in traffic occurs with Malicious Code that simply modifies the victim's DNS server settings or the hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent DNS server replies with "good" answers for most domains. However, when attackers want to direct the victim to a fraudulent site, they simply modify their name server responses. This is particularly effective because the attackers can redirect any of the users requests at any time, and the users would have no idea that this is happening. It is reported that, during December 2005, such an attack was launched against HSBC Brazil, Banco Itau, Banco Banespa and Bradesco banks.
- *Hardware:* During March 2005, police discovered that the London office of the Japanese bank Sumitomo had been the target of a group of hackers for several months. The investigators initially believed that the attackers had used a Trojan. However, after several days of exploration, they found a tiny keystroke-recording device inserted where the keyboard cable connects to the back of the computer. A quick search on the Internet yields a list of a half-dozen companies that sell this type of product.

5.3.4 Identity Theft: Countermeasures

Identity theft is growing day-by-day and people think simple steps such as keeping the credit card and PIN safely will protect them from ID theft. One should be always vigilant and should take optimum care toward protecting the self-identity. Table 5.5 explains some good tips on countermeasures for identity theft.

5.3.5 How to Efface Your Online Identity

Everytime details about your identity and/or about your personal information are revealed on the Internet, you are prone to be a victim for ID theft/fraud. Hence, netizens may think to either protect their identity and/or would like to erase their identity, that is, every footprint available on the Internet. However, it is highly impossible to get one single tool that can completely eradicate each of your footprint from the Internet. Table 5.6 lists few such tools.

Table 5.5 | How to prevent being victim of identity theft

Sr. No.	Security Measures	Brief Description
1	Monitor your credit closely	The credit report contains information about your credit accounts and bill paying history so that you can be tipped off when someone is impersonating you. Watch for suspicious signs such as accounts you did not open. You can also consider identity protection services, which range from credit monitoring to database scanning, for extra security.
2	Keep records of your financial data and transactions	Review your statements regularly for any activity or charges you did not make.
3	Install security software	Install security software (firewall, antivirus and anti-Spyware software) and keep it up to date as a safety measure against online intrusions.
4	Use an updated Web browser	Use an updated web browser to make sure you're taking advantage of its current safety features.
5	Be wary of E-Mail attachments and links in both E-Mail and instant messages.	Use caution even when the message appears to come from a safe sender, as identity information in messages can easily be spoofed (see Appendix C to learn E-Mail security and etiquettes).
6	Store sensitive data securely	Just as you keep sensitive paper documents under lock and key, secure sensitive online information. This can be done through file encryption software.
7	Shred documents	It is important to shred the documents that contain personal or financial information (both paper and electronic) before discarding them. This prevents dumpster diving and, in the online world, the ability for hackers to bypass information that has not been permanently deleted from your system.
8	Protect your PII	Be cautious about giving out your personally identifiable information (PII) to anyone. Find out why the information is needed, and if it's absolutely necessary to give out. Be careful about the details you provide about yourself online, such as on social networking sites.
9	Stay alert to the latest scams	Awareness and caution are effective methods to counter fraud. Create awareness among your friends and family members by sharing security tips you learn with them.

Source: See [44] in References section.

Table 5.6 | How to protect/efface your online identity

<i>Sr. No.</i>	<i>Websites</i>	<i>Brief Description</i>
1	www.giantmatrix.com	Anti Tracks: These are set of tools that appear to be a complete solution to protect your online identity, sensitive data and maintaining the integrity of your system by hiding system's IP address, securely locking and hiding important files and folders and maintaining a healthy system performance, which keeps the system in top-notch condition.
2	www.privacyeraser.com	Privacy Eraser Pro: It protects Internet privacy by cleaning up all the tracks of Internet and computer activities and supports almost all popular web browsers. The main features of this utility are as follows: <ul style="list-style-type: none"> • Erase Browser Cache Files, Browser History, Cookies, Brower Address Bar History and Brower AutoComplete Memory. • File Shredder: Securely shred files and folders. • Cleaning Free Disk Space (Windows FAT/FAT32/NTFS). • Speed up the system.
3	www.reputationdefender.com	MyPrivacy: It removes your personal information such as name, address, age, phone, past address and any other related information. It also helps by continuously monitoring the Internet to remove the footprint available on the Internet.
4	www.suicidemachine.org	Web 2.0 Suicide Machine: It completely roots out your identity from the servers of social networking websites such as MySpace, Twitter and LinkedIn. One will have to reveal the login credentials for the corresponding web applications (webapps) to use this tool. Hence, if he/she does not need them anymore then he/she can let suicide machine eradicate the details from these webapps. It is reported that Facebook have blocked access of Web 2.0 Suicide Machine because Suicide Machine collects login credentials and scrapes Facebook pages. This has been reported as violation of Facebook Statement of Rights and Responsibilities, which has resulted into inability of suicide machine to erase your identity on the Facebook.
5	www.seppukoo.com	Seppukoo: It is an <i>anti-social network</i> failing to destroy your identity, specifically the footprint on the Facebook. The website is named after the "seppuku ritual suicide" practiced by ancient Japanese samurai warriors and the website draws a parallel between restoring a samurai's honor and the "liberation of the digital body." This website is operated by a group that calls itself Les Liens Invisibles, an "imaginary art group from Italy."

SUMMARY

Phishers use different methods and techniques with one common goal of deception, to obtain personal information from the netizens. Phishers have strong technical knowledge and have innovative ideas to deceive the netizens into

1. Believing the messages are received from a trusted source.
2. Believing that the website and/or webpage is a trusted organization and/or institution.

3. Entice the Spam filter to identify that a Phishing E-Mail is legitimate.

Phishing attacks cannot be stopped with any technique and/or technology. However, good practices can reduce the prevalence of Phishing and related losses suffered from Phishing scams.

Phishing is a common form of ID theft in which the netizens are tricked into revealing confidential information about them with economic value. ID theft is increasing day-by-day and awareness and

training is the key to fight against numerous attacks launched to entice the people to reveal their personal information. Besides the countermeasures, one has to be continuously vigilant while disclosing personal information and should evenly treat the risk while disclosing personal information on the Internet, while on the phone or while in person. Many scenarios and case illustrations are provided in Chapter 11 explaining Phishing scams and ID theft.

REVIEW QUESTIONS

1. What is Phishing? Explain with examples.
2. Differentiate between Spam and hoax mails.
3. What are the different methods of Phishing attack?
4. What is Spear Phishing? Explain with examples.
5. What is whaling? Explain the difference between whaling and Spear Phishing.
6. What is identity theft? Explain with examples.
7. How can information be classified?
8. What are the different types of ID theft?
9. What are the different techniques of ID theft?
10. How to prevent being a victim of ID theft?

REFERENCES

- [1] To know more about the world Phishing map, visit: <http://www.avira.com/en/threats/section/worldphishing/top/7/index.html> (25 July 2010).
- [2] Phishing statistics into graphical illustrations can be visited at: http://www.m86security.com/labs/phishing_statistics.asp (25 July 2010).
- [3] To monitor Phishing attacks daily, visit: <http://www.phishtank.com/stats.php> (25 July 2010).
- [4] May 2009 Phishing Report complied by Symantec Security Response Anti-Fraud Team can be visited at: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_05-2009.en-us.pdf (25 July 2010).
- [5] Phishing Activity Trends Report of Q4-2009 published by APWG can be visited at: http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf (25 July 2010).
- [6] To find definition of Phishing, visit: <http://en.wikipedia.org/wiki/Phishing> (9 September 2009).
- [7] To find definition of Phishing, visit: <http://www.webopedia.com/TERM/P/phishing.html> (9 September 2009).
- [8] To find definition of Phishing, visit: <http://www.techweb.com/encyclopedia/defineterm.jhtml?term=phishing> (9 September 2009).
- [9] Visit Phishing attacks launched on most reputed and popular organizations' websites at: <http://www.brighthub.com/computing/smb-security/articles/64477.aspx#ixzz0qFgacNDU> (9 September 2009).
- [10] To know tactics employed by the phisher, visit: <http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx> (9 September 2009).
- [11] Ways to reduce the amount of Spam E-Mails we receive: http://en.wikipedia.org/wiki/E-Mail_spam (2 December 2009).

- [12] To know more about hoax E-Mails, visit: <http://en.wikipedia.org/wiki/Hoax> (5 December 2009).
- [13] To know methods of Phishing, visit: <http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions> (9 September 2009).
- [14] To know more about website Spoofing, visit: http://en.wikipedia.org/wiki/Website_spoofing (5 December 2009).
- [15] To know more about cross-site scripting, visit: http://en.wikipedia.org/wiki/Cross-site_scripting (5 December 2009).
- [16] To know more about cross-site request forgery, visit: http://en.wikipedia.org/wiki/Cross-site_request_forgery (5 December 2009).
- [17] To know more about Phishing techniques, visit: <http://www.brighthub.com/internet-security-privacy/articles/67339.aspx> (26 July 2010).
- [18] To know more about Phishing Net survey, visit: <http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/state-of-the-net-2009/state-of-the-net-2009.htm> (26 July 2010).
- [19] To know more about whaling, visit: <http://netforbeginners.about.com/od/w/f/whatiswhaling.htm> (18 June 2010).
- [20] To know more about Phishing scams, visit: <http://pcworld.about.com/od/emailsecurity/Types-of-Phishing-Attacks.htm> (6 July 2010).
- [21] To know more about Pharming, visit: <http://en.wikipedia.org/wiki/Pharming> (9 September 2009).
- [22] To know more about Phoraging, visit: <http://en.wikipedia.org/wiki/Phoraging> (9 September 2009).
- [23] To know definition of DNS hijacking, visit: http://en.wikipedia.org/wiki/DNS_hijacking (18 June 2010).
- [24] To know definition of DNS hijacking, visit: http://www.pcmag.com/encyclopedia_term/0,2542,t=DNS+hijacking&i=41622,00.asp (18 June 2010).
- [25] To know definition of Click Fraud, visit: http://en.wikipedia.org/wiki/Click_fraud (18 June 2010).
- [26] To know definition of Click Fraud, visit: http://www.webopedia.com/TERM/c/click_fraud.html (18 June 2010).
- [27] To know more about SSL certificate forging, visit: <http://www.symantec.com/connect/blogs/phishing-toolkit-attacks-are-abusing-ssl-certificates> (30 July 2010).
- [28] To know more about search engine optimization (SEO), visit: http://en.wikipedia.org/wiki/Search_engine_optimization (26 July 2010).
- [29] To know more about search engine optimization (SEO), visit: <http://www.securityfocus.com/brief/701> (26 July 2010).
- [30] To know more about techniques used for Black hat SEO attacks, visit: <http://www.net-security.org/secworld.php?id=9084> (26 July 2010).
- [31] To know more on Phishing kits – Xrenoder Trojan Spyware and Cpanel google, visit: <http://www.anti-phishing.info/phishing-kit.html> (30 July 2010).
- [32] How to avoid to be victim of Phishing attack – http://articles.techrepublic.com.com/510010878_115818568.tml?tag=rbxccnbtr1 (2 December 2009).
- [33] To know more on anti-Phishing plug-ins, visit: <http://www.brighthub.com/computing/smb-security/articles/42784.aspx> (8 June 2010).
- [34] To know more about definition of identity theft, visit: http://en.wikipedia.org/wiki/Identity_theft (8 September 2009).
- [35] To know more about identity theft statistics, visit: <http://www.spendonlife.com/blog/2010-identity-theft-statistics> (30 March 2010).
- [36] To know more about identity theft statistics, visit: <http://www.spendonlife.com/guide/2009-identity-theft-statistics> (30 March 2010).
- [37] To know uses of victim information, visit: <http://www.spamlaws.com/id-theft-statistics.html> (18 December 2009).
- [38] To know more about ID theft statistics, visit: <http://www.howstuffworks.com/identity-theft.htm> (2 December 2009).

- [39] To know myths and facts about identity theft, visit: <http://www.networksecurityedge.com/content/ten-common-identity-theft-myths-dispelled> (2 December 2009).
- [40] The article *Identity Theft: The Business Bust-Out'* can be visited at: http://www.businessweek.com/smallbiz/content/jul2007/sb20070723_261131.htm?chan=smallbiz_smallbiz+index+page_top+stories (5 January 2010).
- [41] To know more on business sensitive information, visit: <http://www.businessdictionary.com/definition/sensitive-information.html#ixzz13BzGtac2> (5 January 2010).
- [42] To know more on business identity theft – countermeasures, visit: <http://sbinfo-canada.about.com/od/insurancelegalissues/a/identitytheft.htm> (5 December 2009).
- [43] To know more on medical ID theft, visit: http://www.webopedia.com/DidYouKnow/Internet/2009/medical_identity_theft.asp (9 June 2010).
- [44] To know more on how to protect/eradicate your online identity, visit: <http://www.net-security.org/article.php?id=1366> (5 January 2010).

FURTHER READING

Additional Useful Web References

1. To more about the article *Evolutionary Study of Phishing*, visit: http://www.cc.gatech.edu/projects/doi/Papers/DIrani_eCrime_2008.pdf (26 July 2010).
2. To know more about the article *Learning to Detect Phishing Emails*, visit: <http://www2007.org/papers/paper550.pdf> (26 July 2010).
3. To know more about the article *Detecting Phishing E-Mails by Heterogeneous Classification*, visit: <http://digital.csic.es/bitstream/10261/21694/1/detecting.pdf> (26 July 2010).
4. To know more about the article *What is Phishing?*, visit: <http://antivirus.about.com/od/emailscams/ss/phishing.htm> (6 July 2010).
5. To know more about tabnapping, visit: http://www.computerworld.com/s/article/9177326/Sneaky_browser_tabnapping_phishing_tactic_surfaces (9 July 2010).
6. To know more about tabnapping technique, visit: <http://www.exploit-db.com/papers/13950/> (9 July 2009).
7. To know more about *Security Labs Report*, visit: (January–June 2010): http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_1H2010.pdf (26 July 2010).
8. To know more about the article *There is No Free Phish: An Analysis of “Free” and Live Phishing Kits*, visit: http://www.usenix.org/event/woot08/tech/full_papers/cova/cova_html/ (26 July 2010).
9. Visit DIY Phishing kits introducing new features at: <http://www.zdnet.com/blog/security/diy-Phishing-kits-introducing-new-features/1104> (26 July 2010).
10. To know more about Phishing attacks and countermeasures, visit: <http://www.cert-in.org.in/knowledgebase/whitepapers/ciwp-200-03.pdf> (26 July 2010).
11. To know more on article *How Identity Theft Works*, visit: <http://www.howstuffworks.com/identity-theft.htm> (8 September 2009).
12. To know more on identity theft, visit: <http://www.identitytheft.org/> (8 September 2009).
13. To know more on identity theft, visit: <http://www.321identitytheftnews.com/> (8 September 2009).
14. To know about article *2009 Identity Theft Statistics*, visit: <http://www.spendonlife.com/guide/2009-identity-theft-statistics> (8 September 2009).
15. To know more on article *Your Growing Exposure for Identity Theft Risks*, visit: http://www.idtheft101.net/articles/wiley_rein_white_paper.pdf (26 July 2010).

16. To know about article *NCUA – Guidance on Identity Theft and Pretext Calling*, visit: http://www.ffiec.gov/ffiecinfo/base/resources/info_sec/frb-sr-01-identity_theft_pretext_calling.pdf (26 July 2010).
17. To know about article *Privacy and Identity Theft Conference*, visit: <http://blogs.technet.com/privacyimperative/archive/2008/12/23/privacy-identity-theft-conference.aspx> (27 June 2010).
18. To know about article *Identity Theft and the Internet*, visit: <http://www.student.cs.uwaterloo.ca/~cs492/papers/idTheft.pdf>. (27 June 2010).
19. <http://money.howstuffworks.com/identity-theft4.htm> (Accessed on)
20. To know about article *CID, Mumbai: Phishing Case*, visit: <http://www.cybercellmumbai.com/case-studies/case-of-fishing> (27 June 2010).
21. To know more about identity theft, visit: http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf (27 June 2010).
22. To know more about identity theft, visit: <http://www.nacrc.org/events/annualconfpresentations2005/idtheftnacojuly05.pdf> (27 June 2010).
23. To know more about the article *Identity Theft – Case Studies*, visit: <http://www.id-theft-info.com/Case-Studies.html> (10 June 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Ibid Chapter 29 (*Privacy – Fundamental Concepts and Principles*), Chapter 30 (*Privacy – Business*

Challenges), Chapter 31 (*Privacy – Technological Challenges*) and Chapter 32 (*Web Services and Privacy*).

3. Hayward, C.L. (2004) *Identity Theft*, Nova Science Publishers Inc., USA.
4. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

Articles and Research Papers

1. To read article *Who Is Fighting Phishing*, visit: <http://www.markmonitor.com/download/wpl/wp-fighting-phishing.pdf> (8 June 2010).
2. To read article *MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You*, visit: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (8 June 2010).
3. Dr. Kamlesh Bajaj's scholarly paper *The Cybersecurity Agenda Mobilizing for International Action* is available at: http://www.dsci.in/sites/default/files/cybersecurity_-_mobilizing_for_international_action_0.pdf (28 October 2010). It was presented at the EastWest Institute.
4. Proceedings of “Hack.in 2009” – the 3rd Hacker’s Workshop on Computer and Internet Security, organized by IIT Kanpur, can be downloaded at: http://www.security.iitk.ac.in/hack.in/2009/repository/proceedings_hack.in.pdf (28 October 2010).
5. To know more about article *Stopping Distributed Phishing Attacks* by Alex Tsow, Markus Jakobsson and Filippo Menczer, visit http://archive.nyu.edu/bitstream/2451/15020/2/Infosec+BOOK_Tsow+Jacobson.htm (10 October 2010).

The appendices that serve as extended material for the topic addressed are: A, C, D, E, L, M, O, V. These are provided in the companion CD.

6 | Cybercrime and Cybersecurity: The Legal Perspectives

Learning Objectives

After reading this chapter, you will able to:

- Understand the need for cyberlaws, especially in the Indian context.
 - Understand how the laws of different jurisdictions across the world compare against a single benchmark.
 - Get an overview of the European Union (EU) legal framework for information privacy to prevent cybercrime.
 - Understand legal position on cybercrime with focus on the Indian scenario.
 - Learn the strengths and weaknesses of the Indian IT Act along with the amendment to the Act.
 - Understand Indian IT Act in cybercrime perspective.
 - Understand the meaning of digital signature, public-key infrastructure as well as the implications of digital signature in the context of the Indian IT Act.
 - Learn about electronic records and their admissibility in the courts.
 - Get an overview of challenges faced in punishing the cybercriminals.
 - Understand the Indian challenges in the fight with cybercrime seen from the legal angle.
-

6.1 Introduction

It is said that cybercrime is the *largest illegal industry*. Cybercrime involves massive, coordinated attacks against the information infrastructure of a country. In this chapter, we want to bring forth the point that knowledge of cyberlaws is essential for people who may directly or indirectly interact with networked services either over the Internet or other proprietary networks of businesses and enterprises of any other types – banks, stock brokers, intra-company and inter-company information exchange systems, etc. We have explained the term *cyberlaw* later in this chapter. It is also essential for those who are involved in heavy and indiscretionary use of social networking sites^[1] (e.g., Orkut, Facebook, Big Adda, etc.). We want to understand the meaning of the term *digital evidence* given that the Indian Information Technology Act (ITA) 2000^[2] and its modification (ITA 2008) mention about *evidence*. In the original ITA 2000,^[3] there is a mention about “special provisions as to ‘evidence relating to electronic record’ and ‘admissibility’ of electronic records.” We also explain the legal position on cybercrime based on Section 1.7 of Chapter 1 and discuss the topic of legal aspects of cybercrime into further details. Although the Indian legislations are important for people in India, we must not lose sight of the world scenario – it is important for global businesses. Therefore, while maintaining focus

on the Indian ITA 2000 and subsequent amendments in year 2008, that is, ITA 2008, this chapter also provides an overview of cybercrime legislations in other countries/regions.*

From an Indian perspective, we have provided adequate focus on the Indian ITA 2000 (previously known as the IT Bill) and its recent amendments known as the ITA 2008 (Amendments to the IT Act that came toward the end of year 2008).

Chapter 1 is the background to appreciate the concepts presented in this chapter. An overview on cybercrime is provided in Chapter 1; many fundamental terms with regard to cybercrime are explained (see Box 1.1) in that chapter along with the classification of cybercrime: (a) an Indian perspective on cybercrime is provided in Section 1.7; (b) reference to the Indian IT Act in the context of cybercrime is provided in Section 1.8; (c) a discussion on the global perspective on cybercrime, with implications for organizations and individuals, is available in Section 1.9. With this background, Fig. 6.1 presents the paradigm for cybersecurity.

The concept of *trust seals* mentioned in Fig. 6.1 is a very important one for electronic commerce (E-Commerce) era. (This concept is explained in Ref. #1, Books, Further Reading.) Figure 6.1 shows the *identity theft* group of crimes (identity theft is discussed in Chapter 5). Countries that are members of the EU^[4] (European Union) have very stringent laws for protection of individual privacy and data privacy. (Readers interested in greater details of data privacy should refer to Ref. #2, Books, Further Reading.) The bottom block in Fig. 6.1 points to the IT infrastructure in organizations (government organizations as well as private or other kinds of organizations). From attack perspective, the intrusion detection system (IDS) are important. Readers new to IDS can refer to Ref. #3, Books, Further Reading.

For the benefit of those who are reading this chapter without having referred to Chapter 1, cybercrime definitions are mentioned here as well. Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the

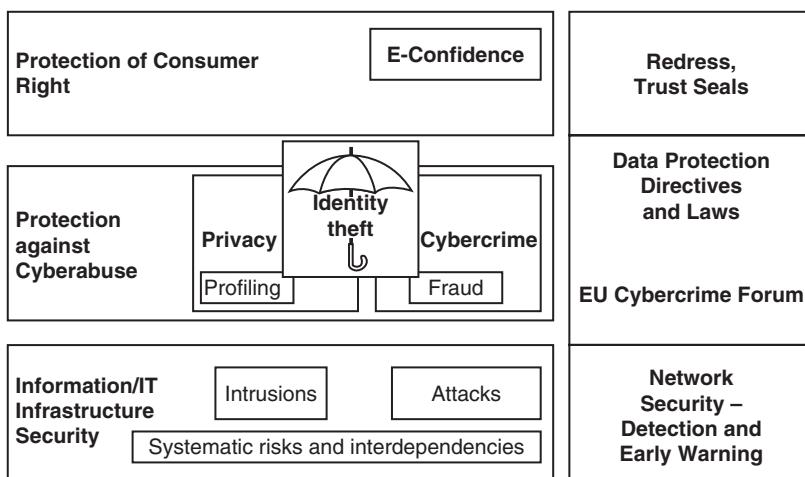


Figure 6.1 | A cybersecurity perspective: European Union.

*caveat – although this chapter provides discussion on the legal aspects of cybercrime, it is important for readers to appreciate that the contents of this chapter are NOT a substitute for consulting the legal experts/legal professionals when a particular case of cybercrime arises with which readers may be confronted or involved with. This is because the legal aspects presented here are based on our awareness and research and by no means, it is claimed to be the perfect or complete knowledge of legal parameters for defending a case. Readers should refer to the paper copy of ITA 2000 and ITA 2008 for exact wordings.

Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined as:

1. **Cybercrime in a restrictive sense (computer crime):** It is referred to any illegal behavior that is carried out by means of electronic methods targeting the security of computer systems and the data processed by them. This can be considered as a narrow definition of the term *cybercrime*.
2. **Cybercrime in a general sense (computer-related crime):** It is referred to any illegal behavior that is committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, and offering or distributing information by means of a computer system or network. This can be considered as a broader definition of the term *cybercrime*.

These definitions are complicated by the fact that an act may be illegal in one nation but not in another. There are more concrete examples, including

1. Unauthorized access to computer (see Box 6.1);
2. causing damage to computer data or programs;
3. an act of computer sabotage;
4. doing unauthorized interception of communications;
5. carrying out computer espionage.

Box 6.1 \ Degrees of Unlawful Access to Computer

In Chapter 1 we mentioned about classification of cybercrimes; one of the cybercrime types mentioned there is unauthorized accessing of computer under the broad category of cybercrime called *cybercrime against property*. Unauthorized access to a computer is most commonly known as *hacking*. Generally, hacking takes place when a person either illegally gains access to a computer system by taking advantage of or overcoming existing security (i.e., passwords and firewalls); or a person exceeds authorized access of a computer. Similarly, *cracking* is when a person gains unauthorized access (or "hacks") into a computer in order to commit a crime within that computer system. From the legal perspective, computer hacking and cracking statutes are titled *Unlawful Access to a Computer*. Such acts are only crimes when done without the consent of the owner. For framing different legal charges, the breakdown of varying degrees of unlawful access to a computer is as follows:

First-degree access: The crime of unlawful access to a computer is of first degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software for the purpose of defrauding or obtaining money, property or services by fraudulent pretense. Such a person is guilty of unlawful access in the first degree. This crime is a *Class C felony*.

Second-degree access: Unlawful access is of second degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software, and the crime results in damages or losses of value considered high enough by the law (the value would vary from country to country). This crime is a *Class D felony*.

Third-degree access: Unlawful access is of third degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software, and the crime results in loss or damage of less than the value that is considered "high" by the prevailing law in the country (this amount varies from country to country). This is a *Class A misdemeanor*.

Fourth-degree access: Unlawful access is of fourth degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software, but there is no loss or damage. This is a *Class B misdemeanor*.

First-degree access is the most serious one from the legal perspective. Relate this to item serial number 5 of Table 1.1 in Chapter 1.

Box 6.1 Degrees of Unlawful . . . (Continued)

Computer trespassing is another term to consider. A person is guilty of computer trespass in the second degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another under circumstances not constituting the offense in the first degree.

In other words, *computer trespassing* involves using a computer with knowledge that such use is without authority and with the intention of: (a) deleting or in any way removing, either temporarily or permanently, any computer data; (b) obstructing, interrupting or in any way interfering with the use of a computer program or data and (c) altering, damaging or in any way causing the malfunction of a computer.

In reference to the above-mentioned term *unauthorized access*, note that the law considers *computer trespass* to be a crime. For example, according to Sections 18.2–152.4 of *Virginia State Criminal Law*, computer trespass is deemed to have occurred when any person uses a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network;
2. cause a computer to malfunction regardless of how long the malfunction persists;
3. alter or erase any computer data, computer programs or computer software;
4. effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
5. cause physical injury to the property of another; or make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by or produced by a computer or computer network shall be guilty of the crime of computer trespass which shall be punishable as a Class 1 misdemeanor.

In the US, as per *Virginia State Criminal Law*, if such an act is done maliciously and the value of the property damaged is \$2,500 or more, the offense shall be punishable as a Class 6 felony. (The term *felony* means an offense or a crime or a criminal act or law breaking/wrong doing.)

All forms of cybercrime are increasing rapidly – cybercrime is the latest and perhaps the most complicated problem in the cyberworld; in a way, it is a bane of Information and Computer Technology (ICT). It is said that the US still produces more malware, Spam and viruses than any other country in the world. Illicit IT jobs are increasingly scattered across an anarchic and international Internet, where labor is cheap, legitimate IT jobs are scarce and scammers are insulated from the laws. Maintaining legal, political and technological standards on the Internet is increasingly important, as cyberattacks take a greater toll. In year 2007, Computer Security Institute in the US conducted a survey^[5] according to which, the average financial loss suffered by individual US corporations, agencies and institutions due to cyberattacks was US\$ 350,424. This loss in figure turns out to be more than double compared to that in the year 2006. Total losses from cyberattacks were \$66.9 million, with financial fraud incurring the most damage at \$21.1 million in total losses. Chapter 1 provided the Indian statistics on cybercrime (refer to Tables 1.1–1.4). This is the background for understanding the legal landscape on cybercrime.

6.2 Cybercrime and the Legal Landscape around the World

Before getting into India-specific discussion, we discuss here the world scenario considering the following countries: the US, Europe, Canada, Asia-Pacific and Africa. First, let us examine the term *crime* under the legal microscope. *Crime* is a legal concept and has the sanction of the law. Crime or an offense is “*a legal*

wrong that can be followed by criminal proceedings which may result into punishment.” The hallmark of criminality is that it is breach of the criminal law. Box 6.1 describes various scenarios for the unlawful access to a computer system. We start with a broad view of the legislative analysis in the Asia-Pacific region, followed by a detailed examination of the legal status (with regard to cybercrime and privacy protection) in Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, Thailand, South Korea and Vietnam. From this discussion we will realize that the extent and nature of Internet safety, security and privacy legislation in the Asia-Pacific region varies widely. We will also have a discussion on federal laws in the US about cybercrime. Next, we will discuss the EU legal framework to prevent cybercrime.

One of the preconditions for development of the Information Society is for users to have confidence or “trust” in the reliability, security and integrity of electronic communications systems and computerized information processing systems. This is supported by much literature; for example, the work by researchers at the Carnegie Mellon University in their research paper *The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study* (accessible at the link <http://weis2007.econinfosec.org/papers/57.pdf>) Individuals will be reluctant to use networks or systems they do not trust. If there is no trust, individuals will tend to either not disclose personal information or provide false information. Therefore, one critical component of the trust framework is *privacy protection* – the provision of assurances by means of law, technology design and industry practice that personal information will be collected, exchanged and used fairly. As far as the law is concerned, the Web, that is the World Wide Web (WWW), still resembles the *wild west*. Bringing about legal governance for behavior on the Web is a specialty evolving rapidly due to innovations on the Internet. Catching cybercriminals under the legal edifice is a challenge. This is so partly because there is “no central authority” that enforces cyberlaw when crimes are committed. Plaintiffs still turn to traditional law enforcement to solve problems.

6.2.1 A Broad View on Cybercrime Law Scenario in the Asia-Pacific Region

When we consider challenges involved in the Asia-Pacific region, for handling cybercrime, we realize that the challenges exist mainly due to the general lack of awareness of information security issues, the rapidly evolving complexity, capacity and reach of ICT, the anonymity afforded by these technologies and the trans-national nature of communication networks. Consequently, only a few countries of the Asia-Pacific region have appropriate legal and regulatory frameworks to meet these challenges. Even where awareness is growing and where legislation may be adequate, capacity to use information security technologies and related procedures as well as to protect against, detect and respond effectively to cybercrime, and to assist other countries, is low. As a result, published cybercrime reports may represent only a small fraction of their incidence and there is a need for more accurate estimates of the prevalence of cybercrime.

Information privacy or data protection in this context is not about keeping personal information secret; rather, it is about creating a trusted framework for collection, exchange and use of personal data in commercial and governmental contexts. The *Fair Information Practices* (FIPs) are explained in detail in Ref. #4, Books, Further Reading. Data protection laws^[6] permit, and even facilitate, the commercial and governmental use of personal data while providing to individuals (a) control over what to disclose, (b) awareness of how their personal data will be used, (c) rights to insist that data are accurate and up to date, and (d) protection when personal information is used to make decisions about a person.

Now let us consider the Australian Cybercrime Act 2001. The Australian Cybercrime Act 2001 came into effect in Australia in April 2002. This was the third time that a Federal Government has passed cybercrime legislation; previous legislation was passed in 1989 and in 1995. Each attempt was meant to reduce the gap between legislation and malicious online activity. However, Cybercrime Act 2001 is the subject of much

controversy as critics argue that it is too broad in jurisdiction, extends police powers too far and threatens to facilitate the unjust conviction of many Information Technology (IT) professionals. This Act provides too broad a definition of *cybercrime*. Much of the criticism is based on that excessively broad definition and the extent to which the Act has been left for interpretation by the courts. Let us take a glimpse of the Australian Cybercrime Act 2001. This Act introduces the following new offenses to the Criminal Code Act 1995.

1. The serious offenses under Division 477 are as follows:
 - *Section 477.1:* Unauthorized access, modification or impairment with intent to commit a serious offense.
 - *Section 477.2:* Unauthorized modification of data to cause impairment.
 - *Section 477.3:* Unauthorized impairment of electronic communication.
2. The other offenses under Division 478 are as follows:
 - *Section 478.1:* Unauthorized access to, or modification of, restricted data.
 - *Section 478.2:* Unauthorized impairment of data in a computer disk, etc.
 - *Section 478.3:* Possession or control of data with intent to commit a computer offense.
 - *Section 478.4:* Producing, supplying or obtaining data with intent to commit a computer offense.

Not surprisingly, the Australian Cybercrime Act 2001 has drawn considerable criticism: it criminalizes far too much and far too easily, leading to severe consequences for IT professionals. This problem arises primarily from the overly broad definitions adopted by this legislation, specifically the breadth of the terms defined (in the Cybercrime Act) has created an even broader scope of potential criminality. Among the most concerning aspects of the Act are the definitions of *restricted data* and *authorization*; the mental elements of the offenses and the actions that constitute an offense: unauthorized access, modification and impairment.

1. **Restricted data:** In order for data to be defined as *restricted*, it simply needs to be held in a computer that uses an access control system. However, it is NOT a requirement that the data itself is protected by an access control system; only the computer needs to be protected by the access control system. According to this definition, the requirement of *restricted data* can be too easily met, as almost all computers are protected by at least a password. Therefore, to be in breach of Section 478.1 of the Australian Cybercrime Act 2001, an individual simply needs to view almost any data without authorization, notwithstanding whether or not that data was secured. This is further complicated by the lack of explanation of what constitutes having “authorization.”
2. **Authorization:** A key requirement for conviction, under any of the Division 477 offenses and half of the Division 478 offenses, is that access, modification or impairment is undertaken without “authorization.” Yet the Australian Cybercrime Act merely states that the action undertaken must be unauthorized, without actually specifying what constitutes authorization. The Act does not, in any way, address situations where authorization may be disputed, revoked or granted conditionally. For example, if an IT professional is hired to undertake some work, and suppose that in the course of that work, the authorization granted to that person is disputed or revoked, then there may exist a basis for prosecution under Section 478.2 (of the Australian Cybercrime Act 2001) for “unauthorized access or modification to restricted data.” The additional requirement of *restricted data* can be easily met, as explained above.

Now let us understand the powers granted by the Australian Cybercrime Act. Under the Act, new powers granted for law enforcement include:

1. The power to remove “a thing” to another place for the purpose of examination or processing to determine whether it may be seized under a warrant, if it is more practical, or there are reasonable grounds that the “thing” includes or is an evidence.

2. The power to “operate electronic equipment” at the warrant premises in order to access data (including data not held at the premises) if the police believe that the data (may) contains evidentiary material.
3. The power to require a person “to provide any information or assistance” that is considered reasonable and is necessary in order to allow the officer to make a copy of data from equipment that might contain evidential material.
4. The power to require a “person with knowledge of a computer or a computer system to assist access,” etc.

In conclusion, we note that the enactment of the Australian legislation means that it is now possible that other well-intentioned actions by Australian IT professionals may be regarded as criminal activities. IT professionals must now take more care in the performance of their duties, and must be much more aware of how their actions may be construed, to avoid risk of prosecution for their well-intentioned actions. The Australian Cybercrime Act 2001 heralds an era of de facto censorship in research and development of computer science fields.

6.2.2 Online Safety and Cybercrime Laws: Detailed Perspective on the Current Asia-Pacific Scenario

The extent and nature of Internet safety, security and privacy legislation in the Asia-Pacific region varies widely. In this section, we are going to consider the legislative position in Asia-Pacific countries with regard to data privacy (impacted by most forms of cybercrimes such as, e.g., identity theft), Spam (unwanted mails) and online child safety (because this closely relates to COPPA). Our objective in this section is to gain an understanding of how the laws of different jurisdictions compare against a single benchmark. In some areas such as computer security laws and online child safety laws [such as the Children’s Online Privacy Protection Act (COPPA),^[7] also mentioned in Chapter 1)], there exist international norms on the best approach to regulation. For example, the Council of Europe’s (CoE’s) Convention on Cybercrime is widely regarded as the international norm on the criminalization of computer-related conduct, and the International Centre for Missing and Exploited Children (ICMEC) has developed authoritative model legislation that criminalizes the production of, and certain dealings with, child pornography.^[8] This model has been adopted as the benchmark legislation for the computer security and online child safety matters. However, in other areas, such as privacy laws and Spam, there seem to be no international norms.

In the privacy arena, there are numerous regional norms, such as the *Asia-Pacific Economic Co-operation* (APEC) Privacy Framework and the EU’s Data Protection Directive, but an international consensus on the best approach to data protection regulation has not yet been reached. However, CoE’s Convention on Cybercrime^[9] serves as the benchmark legislation (see Box 6.2). Titles 1, 2 and 5 of the CoE’s Convention on Cybercrime serve as the benchmark legislation. The alignment status of various Asia-Pacific countries mentioned in Table 6.1 is in that benchmark reference.

Box 6.2 The APEC Framework on Privacy

Today belongs to “global economy” and information flows are vital to conducting business in a global economy. The APEC Privacy Framework promotes a flexible approach to information privacy protection for APEC Member Economies, while avoiding the creation of unnecessary barriers to information flows. The APEC Privacy Framework is a practical policy approach to enable accountability in the flow of data while preventing impediments to trade. It provides technical assistance to those APEC economies that have not addressed privacy from a regulatory or policy perspective.

Box 6.2 The APEC . . . (Continued)

The framework will enable regional data transfers to the benefit of consumers, businesses and governments. The framework provides clear guidance and direction to businesses in APEC Member Economies on common privacy issues and outlines the impact of these issues on the various legitimate business models. It does this by outlining reasonable expectations of the modern consumer on how their privacy interests should be protected.

There are nine principles to the APEC Privacy Framework:

1. Preventing harm;
2. integrity of personal information;
3. notice;
4. security safeguards;
5. collection limitations;
6. access and correction;
7. uses of personal information;
8. accountability;
9. choice.

Data is the digital currency that fuels the growth in many of today's economies. This framework will facilitate responsible information flows, which creates an essential basis for increased trade and E-Commerce to flourish. It enables government, business and societal benefits by developing domestic markets, improving efficiencies and economic growth, and attracting foreign investment, which also leads to developing local industry. The framework focuses on both domestic and international implementation of privacy standards for APEC Member Economies. It explores new ways of information sharing and cooperation across agencies and authorities to enable transfers of personal information across borders. The framework also provides specific examples of privacy situations and focuses its attention on practical and consistent information privacy protection within this context. The framework balances privacy with all relevant interests while according due recognition to issues of cultural and economic diversity that exist within the APEC Region.

Note: Privacy details are discussed in detail in Ref. #4, Books, Further Reading.

Computer Security Laws

The Australian, New Zealand, Singaporean, Taiwanese and Thai Governments have each enacted robust computer security laws that cover most of the core and computer-related offenses found in the CoE's Convention on Cybercrime. The computer security laws in China, Hong Kong, Japan and South Korea are moderately aligned with the Convention. The enacted laws in Malaysia, the Philippines and Vietnam are moderately to weakly aligned, respectively, with the Convention (see Table 6.1). Malaysia and the Philippines have enacted some computer security offenses; however, the focus of these offenses appears to be on unauthorized access and these countries still rely on their general law to criminalize a number of the acts prohibited by the Convention. Vietnam's implementation of the Convention's core, and computer-related fraud and forgery, offenses appears to be piecemeal and arises from the enactment of multiple, overlapping prohibitions in various instruments, including the Law on Information Technology 2006 and the Law on E-Transactions 2005.

In India, although the ITA 2000 prohibits many of the activities that constitute core offenses under the Convention, the IT Act does not, for the most part, criminalize these activities – it merely provides for significant liability in damages. This civil liability approach is unique in the region. India's Information Technology (Amendment) Bill 2006 (IT Amendment Bill No. 96 of 2000) was proposed to amend the IT Act to criminalize many of the Acts that constitute core offenses under the Convention but only where they are done "dishonestly or fraudulently." In September 2007, the Standing Committee on IT submitted its

Table 6.1 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to the benchmark legislation

Favorable Alignment	Moderate Alignment	Weak Alignment
Australia	China	India
New Zealand	Hong Kong	Indonesia*
Singapore	Japan	—
Taiwan	Malaysia	—
Thailand	Philippines	—
—	South Korea	—
—	Vietnam	—

*No computer security laws have been enacted.

report on the IT Amendment Bill to address a number of substantive recommendations in respect of the bill. This resulted in the ITA 2008 (amendments to the Indian ITA 2000).

Indonesia's Bill on Electronic Information and Transaction (EIT) is weakly aligned with the Convention (refer to Table 6.1). Partly, this is due to its emphasis on unauthorized access and the protection of government and financial computer systems. Japan and China have also been considering updated cybercrime laws for some time now. The Japanese parliament, since 2004, has a long pending matter of amendment to the criminal code to criminalize the preparation, production, dissemination and use of computer viruses and malware; this has been pending along with a separate piece of legislation that seeks to implement Japan's remaining obligations as a signatory to the Convention on Cybercrime. China has drafted its "National Information Security Regulations." However, neither the content of these regulations nor the timeframe for their enactment is known. Table 6.1 shows the alignment position of the mentioned countries with regard to the CoE's Convention on Cybercrime as the benchmark.

This degree of alignment varies due to the range of Convention offenses covered by the enacted legislation and the restrictive way in which some of the Convention offenses are implemented (e.g., requiring that unauthorized access be obtained by use of a telecommunications line). Take the example of Hong Kong – its general criminal law seems to apply in several cases to computer-facilitated act that is criminalized by the Convention on Cybercrime. It is interesting to know that Hong Kong has enacted fewer offenses with regard to computer security, which is one of the aims to which the Convention is directed. Owing to lack of comprehensive computer security laws, jurisdictions such as Indonesia rely on the application of their existing laws to regulate conducts that are declared criminal by the Convention. Legislatures in Indonesia, India and the Philippines are currently considering comprehensive computer security laws. In India, as we know the IT Act has been amended. The Philippines' proposed Cybercrime Prevention Act of 2005 (HB 3777) is considered to be the most closely aligned with the Convention on Cybercrime. It almost identically reproduces the Convention's core offenses, computer-related fraud and forgery offenses, and ancillary liability provisions.

Data Privacy and Data Protection

Position on privacy laws also greatly varies in the Asia-Pacific region. Table 6.2 shows the alignment position with regard to the benchmark legislation that was mentioned earlier in this discussion. The Microsoft-drafted Model Privacy Bill serves as the benchmark legislation in data privacy arena (referred to as the *Model Bill*). Privacy mature organizations are regulated by prevailing privacy regulations in their respective countries. As such, and as per the FIPS, these organizations must provide a "privacy notice" before collecting "personally identifiable information" (PII). *Privacy notice* is a statement made to a data subject that describes how the

Table 6.2 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to Microsoft Model Privacy Bill

Favorable Alignment	Moderate Alignment	Weak Alignment
—	Australia	India*
—	Hong Kong	Indonesia*
—	Japan	Malaysia
—	New Zealand	Philippines
—	—	Singapore*
—	—	South Korea
—	—	Taiwan
—	—	Thailand
—	—	Vietnam

*No data protection laws have been enacted.

organization collects, uses, retains and discloses personal information. Sometimes, a privacy notice is referred to as a privacy statement, a fair processing statement and even a privacy policy. Providing privacy notice is important to be entitled to use or disclose it for a secondary purpose. The privacy-regulated organization must obtain a prior consent of the data subject – either explicit, Opt-Out or implied – depending on several factors related to the privacy risk involved (see Fig. 6.2).

From privacy perspective, there are two kinds of information about individuals: *aggregated information* and *PII*. Aggregate information or statistical information is complied, that is not personally identifiable. Examples of aggregate information include, but are not limited to, demographics, domain names and website traffic counts. PII is any information that can be traced to a particular individual. Note that *aggregate information* is not considered as PII. For example, information indicating the number of visitors to a particular Internet site. Commonly known examples of PII are the “social security number” (SSN) in USA, personal account number (PAN) in India, name, E-Mail address, phone number, etc. Personal user preferences tracked by a website via a cookie are also considered personally identifiable when linked to other PII provided by a user online. The definition of PII may vary from organization to organization. Some people in the IT industry

Opt-In is a process in which personal information will be processed *only if* the data subject indicates it should be so.

An *Opt-In* is considered to be an *explicit* consent

Opt-Out is a process in which personal information will be processed *unless* the data subject indicates it should be otherwise.

An *Opt-Out* is considered to be an ‘*implicit*’ consent

Related Concepts

Subscribe/unsubscribe Register/unregister double Opt-In

Examples

Yes, Please include me.....(user needs to uncheck the box if he/she does not wish to be included)

Yes, Please include me ... (user needs to check the box if he/she does not wish to be included)

Figure 6.2 | Opt-In and Opt-Out.

believe that a *dynamic* IP address is NOT a PII because it varies depending on which computer network one is connected to, whereas a *static* IP address is a PII because it is always fixed. *Privacy notice* is considered as a mature privacy practice in organizations.

There are several protected disclosures to which the Model Bill's provisions relating to use and disclosure of PII do not apply. These non-applicability situations include the scenarios where the disclosure is made to service providers and related companies that operate under a common set of internal policies. The Model Bill also contains access and correction as well as security-related provisions, including a breach notification obligation. The breach notification is triggered when a security breach results in (or it is likely that a breach will result in) the misuse of a resident's unencrypted sensitive financial information. Table 6.2 shows alignment position of Asia-Pacific countries with regard to Microsoft's Model Privacy Bill as the benchmark.

According to Organization for Economic Co-operation and Development (OECD) "Guidelines on the Protection of Privacy and Trans-border Flows,"^[10] the data protection laws in Australia, Hong Kong and New Zealand are moderately to favorably aligned with the benchmark legislation. The strengths of these regimes vis-à-vis the Model Bill include their broad application to the private sector and their notice, security and access provisions. There is one aspect of the Model Bill that these regimes have not adopted in full – it is the tiered consent model that takes account of the privacy risk inherent in secondary use or transfer (i.e., a model that imposes more onerous consent requirements where the associated privacy risk is greater). Furthermore, the imposition of restrictions on transborder data flows in Australia and Hong Kong are deviations from the Model Privacy Bill.

If we consider on its own, Japan's Act Concerning the Protection of Personal Information appears to be moderately aligned with the benchmark legislation. Yet, it is possible that the sectoral guidelines to explain the application of the Protection of Personal Information in certain industry sectors may alter this analysis. OECD Guidelines are used by South Korea's data protection regime as well; however, the South Korean data protection regime is less well aligned with the benchmark legislation. South Korea's alignment with the Model Privacy Bill is impacted by a combination of restrictive provisions in the legislation, such as requiring a data subject's consent for transborder data flows within a corporate group, and the way in which the legislation has been interpreted and enforced by the Korea Information and Security Agency (KISA).

Taiwan's Computer-Processed Personal Data Protection Law has limited applicability to certain industries in the private sector. The Taiwanese Law is unique in the region as long as it establishes a mandatory licensing regime for the regulated entities that collect, use or disclose personal data. Thailand does not have legislation for private sector data protection. However, the Official Information Act 1997 does regulate state agencies for dealings with personal information. Vietnam does not seem to have any comprehensive data protection laws of general application. However, the Vietnamese Law on Information Technology 2006 does contain a limited data protection provision applicable to the collection, use and disclosure of personal information in a networked environment. In the E-Transactions Law, there are similar provisions to address the handling of personal information collected as part of an electronic transaction – a very common phenomenon in E-Commerce paradigm. The Philippine Department of Trade and Industry has recently come out with an administrative order with guidelines to protect personal data held by private sector organizations. These voluntary guidelines are a measure of a different kind to the Model Bill; they aim at encouraging private sector organizations to adopt privacy policies rather than penalizing them for not doing so.

Malaysia (as at the time of writing this) does not have a comprehensive data protection legislation. However, the General Consumer Code developed following the Communications and Multimedia Act of 1998, contains provisions toward the protection of personal information collected by licensed telecommunications service providers. China, India, Indonesia and Singapore have not enacted data protection legislation per se. China, India, Indonesia, Malaysia, South Korea, Taiwan and Thailand are currently considering data protection legislation (as the time of writing this). APEC Privacy Framework in 2005 has served as the trigger for reform in this area.

The Taiwanese legislative proposal, when enacted, would bring the country's existing regime more into line with the ideal advocated by the benchmark legislation. The position in South Korea is not so clear; as at the date of writing this, it is understood that the South African Government has plans to consolidate three of their private sector instruments that were previously meant for consolidation into a single bill. The Indonesian and Indian data protection proposals are only minor parts of pending cybercrime legislation. Toward that, in September 2007, India's Standing Committee on IT recommended that India enact a more comprehensive data protection regime as part of the proposed amendments to the IT Act discussed in the computer security section previously.

For a long time, Malaysia, Thailand and China have been contemplating to have a legislation toward data protection. The most recent publicly available draft of the Malaysian legislation contemplated a model similar to Hong Kong's Personal Data Privacy Ordinance, which would stand the pending legislation in good stead vis-à-vis the Model Privacy Bill. It is understood that a further draft of Malaysia's data protection legislation has been prepared since then. The Thai Government is presently considering ways to come closer toward its proposed alignment with the APEC Privacy Framework. China's State Council Normalization Office is in discussions with data protection experts to finalize the content of their proposed legislation which was placed on the National People's Congress legislative agenda in 2008.

Spam Laws

The checklist drafted by Microsoft contains features of effective anti-Spam legislation. It is considered as the benchmark legislation for this part of the discussion. The Microsoft checklist envisages an "Opt-Out" anti-Spam regime to address commercial electronic messages. However, the checklist mentions that transactional or relationship messages (such as messages sent to customers with regard to products or services purchased from the sender) should be excluded from the scope of regulation, as it should contain messages that only have an incidental commercial purpose. The Microsoft checklist contains the usual restrictions on transmitting electronic messages of commercial nature – without an unsubscribe facility or accurate sender and header information – and provides that customers should be able to Opt-Out from the receipt of commercial electronic messages on a product-line basis as well as on a company-wide basis. However, the checklist does not contemplate any "ADV" or other labeling requirement. Effective anti-Spam legislation needs to also include strong antiaddress harvesting and dictionary attack measures, as well as service provider liability provisions that preserve the right of Internet Service Providers (ISPs) and E-Mail service providers to fight against Spam. As far as enforcement is concerned, the Microsoft checklist contemplates enforcement by ISPs, E-Mail service providers and the government. The available remedies should include: (a) civil liability in damages, (b) capped statutory damages that may be adjusted to take into account willful violations and implementation of best practice procedures and (c) criminal sanctions for intentional and unauthorized acts, including those involving fraud.

In recent times, there has been a discernible move in the Asia-Pacific region toward the enactment of anti-Spam legislation. There are now seven countries in this region that have enacted comprehensive anti-Spam legislation: Australia, China, Hong Kong, Japan, New Zealand, Singapore and South Korea. Of these, Hong Kong's Opt-Out regime appears to be the most closely aligned with the checklist, with Australia and New Zealand being positioned not too far behind despite implementing Opt-In models. Singapore has enacted an Opt-Out regime with "bulk" and labeling requirements, whereas the requirements of South Korea's regime vary depending on the medium by which the advertising is transmitted. China's Internet E-Mail Service Management Regulations 2006 are moderately to weakly aligned with the checklist due in part to their application only to E-Mails and their "AD" labeling requirement. Hong Kong and New Zealand are currently the only jurisdictions in the region that explicitly exclude transactional or relationship messages from the scope of regulation.

Philippines, Thailand and Vietnam have enforced anti-Spam measures that are less comprehensive. The broadcast messaging rules implemented in the Philippines are considered as an interim measure designed to address a particular area of concern, namely, Spam SMS and MMS, pending the development of a more comprehensive regime. Thailand chose to enact Spam-related provisions as part of its 2007 computer security legislation. Those provisions are likely to have limited application to Spam that is not fraudulent or designed to interfere with the operation of the recipient's computer system. Two sources of Spam-related obligations are available in Vietnam: (a) the Law on Information Technology 2006 and (b) Decree 142 Specifying Administrative Penalties in the Field of Post, Telecommunications and Radio Frequency. These instruments address "advertisement information" transmitted over networks and "unsolicited messages," respectively. However, neither instrument brings about a comprehensive Spam regime. In the absence of specific anti-Spam legislation, jurisdictions such as India, Indonesia, Malaysia and Taiwan rely on their existing computer security and/or consumer protection laws to regulate Spam activity. In a way, this approach succeeds toward eliminating the consequences of Spam activity; it is increasingly being accepted by legislatures in the region that specific anti-Spam legislation is necessary to reduce Spam volumes.

Legislatures in India, Indonesia, the Philippines and Taiwan are currently considering anti-Spam legislative proposals. Of these proposals, Taiwan's "Opt-Out" legislation appears to be the most advanced in the legislative process, as well as being the most closely aligned with the checklist (the meaning of the term "Opt-Out" has been explained earlier; see Fig. 6.2). In India, the definition of *unsolicited commercial communications* is presently defined and is based on Opt-Out approach solicited by the Reserve Bank of India, that is, those customers who do not want to receive unsolicited commercial communications.

Vietnam's inter-agency taskforce is at an early stage of drafting a diktat on Spam. A draft of the diktat was expected in late 2007. The pending computer security laws in India, Indonesia and the Philippines contain Spam-related provisions. If enacted in their current form, the Spam-related provisions in India's IT Amendment Bill is to apply only to certain limited types of Spam and not mere unsolicited commercial electronic messages. In its report on the IT Amendment Bill, the Standing Committee on IT questioned whether these provisions contained a sufficient response to the problem of Spam. The Committee recommended that India enact specific anti-Spam legislation.

Box 6.3 India and Anti-Spam Legislation

A few years ago, Bill Gates proclaimed that Spam would no longer be a problem in 2006. However it did not happen. Spam is nothing but unsolicited bulk E-Mail (UBE) or unsolicited commercial E-Mail (UCE). Note that Spam is "unsolicited" which means that there is no prior relationship between the parties concerned and the recipient has not explicitly consented to receive the communication. Unsolicited E-Mail, also called "Spam," is a growing concern among corporations and individuals. Spamming was once viewed as a mere nuisance – it is now posing alarming problems. Way back in 2002, losses to US Corporations due to Spamming were a staggering \$8.9 billion. In 2003, Spam costs to all non-corporation Internet users were an estimated \$255 million. With the increasing number of Internet users in India, the absence of any legislation prohibiting Spamming and the dearth of other Spam-control measures, it is time the government took note of this menace.

Spam legislation is non-existent in India. The ITA 2000 does not discuss the issue of Spamming at all. It only refers to punishment for those, who after having secured access to any electronic material without the consent of the person concerned, disclose such electronic material to any other person. It does not have any bearing on violation of individual's privacy in cyberspace. The illegality of Spamming is not considered. The Delhi High Court acknowledged the absence of appropriate legislation concerning Spam in a recent case wherein Tata Sons Ltd and its subsidiary Panatone Finwest Ltd filed a suit against McCoy Infosystems Pvt Ltd for transmission of Spam. It was held that in the absence of statutory protection to check Spam mails on Internet, the traditional tort law principles of trespass to goods as well as law of nuisance would have to be used.

Box 6.3 India and Anti-Spam . . . (Continued)

Spam is harmful because for a number of reasons as follows:

1. **Content:** Most of the objections to Spam come up due to its content. Commercial messages may promote dubious ventures; sometimes messages with sexually explicit material are commonplace. However, the most important objection to Spam messages is that they may contain harmful embedded code and hostile file attachments.
2. **Internet resources consumed:** A significant proportion of all E-Mail traffic constitutes of Spam, resulting in massive consumption of network bandwidth, memory, storage space and other resources. Internet users and system administrators spend a great deal of time reading, deleting, filtering and blocking Spam, as a result of which they pay more for Internet access.
3. **Threat to Internet security:** Spammers frequently tap into Simple Mail Transfer Protocol (SMTP) Servers and direct them to send copies of a message to a long list of recipients. Third-party relaying usually represents theft of service because it is an unauthorized appropriation of computing resources. A company's reputation may be damaged if it is associated with Spam because of third-party relaying.

The legal methods to deal with the Spamming menace are prohibition, enforcement of anti-Spam policies, Opt-Out clause, statutory provisions and enforcement mechanisms. Although there are legal methods to deal with Spam, there is considerable debate whether we need to prohibit or restrict Spam? Even if one assumes that Spam is bad, there are many countervailing issues that must be analyzed with regard to any legislation that prohibits or restricts Spam. These countervailing issues include the following:

1. Civil liberties advocates say that there are constitutional issues to consider which could trickle down to other types of speech over the Internet. Furthermore, different countries have different free speech laws. What may be legal in one country may be entirely unlawful elsewhere. In India, there are strong and explicit freedom of speech protections; the Supreme Court has held commercial advertising to be an inalienable part of freedom of speech which is enshrined in Article 19 of the Constitution. This is the reason why some legislators and advocates argue that the anti-Spam legislation has to be very specific in that the proposed legislation has to truly limit itself to only "commercial E-Mail."
2. Consumer protection laws exist to protect the consumer from fraudulent and deceptive advertising.
3. Legislation prohibiting pornography already exists although some modification to such legislation may be required, so that Internet users have some protection from receiving pornographic materials via Spam.

Indonesia's EIT Bill does not propose to regulate Spam messages per se. Instead, the EIT Bill proposes to require eSellers (i.e., persons who offer to sell goods and services offered through electronic media) to provide complete and correct information in relation to the terms of the contract, the good or service offered and the producer of the good or service. The Spam-related provisions in the Philippines' Cybercrime Prevention Act of 2005 (HB 3777) propose to establish a basic Opt-Out regime (refer to Fig. 6.2). Plans are afoot to amend Japan's law regarding the regulation of transmission of specific E-Mail. The Ministry of Internal Affairs and Communications was to submit a bill to the The National Diet of Japan (Japan's bicameral legislature) in 2008. The Bill was to create an Opt-In regime for Spam E-Mails accessed from computers and mobile phones. Malaysia and China may also enact anti-Spam laws in the future. There was an announcement in August 2007 by the Malaysian Communications and Multimedia Commission saying that it had issued a tender for the provision of consultancy services for studying legislative responses and drafting anti-Spam legislation for Malaysia. As for China, it is understood that the Internet Society of China, supported by the Ministry of Information Industry, is engaged in research to look into various possible approaches toward comprehensive Spam legislation. Draft codes of practice are under consideration in both Hong Kong and New Zealand. These codes of practice are expected to provide regulated entities with further guidance on how to comply with the comprehensive

Table 6.3 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to anti-Spam laws (Microsoft checklist)

Favorable Alignment	Moderate Alignment	Weak Alignment
Hong Kong	Australia	India*
—	China	Indonesia*
—	New Zealand	Malaysia
—	Singapore	Philippines
—	South Korea	Taiwan*
—	—	Thailand
—	—	Vietnam

*No Spam laws have been enacted.

anti-Spam regimes that have recently been enacted in Hong Kong and New Zealand. Table 6.3 presents the alignment position of Asia-Pacific countries with regard to the Microsoft checklist for anti-Spam legislation.

Online Protection for Children

This is closely related to COPPA (refer to Chapter 1). For readers' reference, ICMEC stands for International Centre for Missing and Exploited Children. A combination of the child pornography offenses in Title 3 of the Convention on Cybercrime and the core elements of ICMEC's Model Child Pornography Legislation serve as the benchmark instrument for this part of the analysis. The child pornography offenses in Title 3 of the Convention of Cybercrime aim to circumscribe the use of computer systems in the commission of sexual offenses against children. As such, the Convention requires signatories to criminalize acts such as the production of child pornography for the purpose of its distribution through a computer system, and offering, making available, distributing or transmitting child pornography through a computer system. Being in possession of child pornography material in electronic form stored in a computer system is also subject to criminalization. In ICMEC's view, effective child pornography legislation must specifically apply to child pornography and not just pornography in general. Therefore, the legislation must include a definition of child pornography (where a child is a person under the age of 18 irrespective of the age at consent to sexual relations). In an effective child pornography, legislation should also expressly criminalize the possession of child pornography regardless of the intent to distribute, and require ISPs to bring to the notice of relevant authorities all suspected child pornography matters.

Online child safety laws are among the least developed in the region vis-à-vis the benchmark legislation. Most countries have enacted broad obscenity regimes that have some application to online dealing in child pornography. There are only 5 of 14 jurisdictions, namely, Australia, Hong Kong, Japan, South Korea and Taiwan, which have enacted legislation to specifically address child pornography. Three of the fourteen jurisdictions, that is, Australia, Hong Kong and Taiwan, have enacted legislation on computer-facilitated child pornography offenses. The specific child pornography legislation, enacted in the region, generally adheres to the applicable ICMEC principles; however, only Australia and Hong Kong criminalize mere possession of child pornography (i.e., possession, irrespective of the intent to distribute). The computer-facilitated child pornography offenses enacted in Australia, Hong Kong and Taiwan cover most of the prohibited acts under Title 3 of the Convention; Australia is the only jurisdiction in the region to impose an obligation on ISPs and content hosts to report material that they reasonably believe to be child pornography material (a similar provision exists in the US law). Although New Zealand has not enacted specific legislation to combat child pornography, case law confirms that New Zealand's classification regime does apply to child pornography, and certain of the offenses under that regime attract more serious sanctions where the offending publication

promotes sexual exploitation of children, among other things. The Thai Computer Crime Act criminalizes certain computer-facilitated dealings with pornography, it does not specifically refer to child pornography.

Although child pornography is now being touted as a global issue, there is no legislation in India, Indonesia, Malaysia, the Philippines, Singapore and Vietnam to specifically address child pornography. However, the absence of specific child pornography legislation in these countries needs to be understood in the context of these countries' approach to control pornographic content. For example, in some of the Asia-Pacific jurisdictions, such as Malaysia, Singapore and Vietnam, the ISPs are primarily held responsible for control of content as well as hosting of content. However, in Vietnam this responsibility lies with the state, society and schools. As such, these entities will be held responsible if obscene material is transmitted using their services. With this approach to control of content, the need for specific legislation to eradicate child pornography is not perceived as necessary because it is believed that the approach serves to reduce the availability of child pornography online.

Currently, the Philippine, Indian, Indonesian and Japanese legislatures are considering online child safety laws. ITA 2008 addresses child pornography. Most of these pending laws are subsumed in the broader proposals to enact computer security laws. The Philippine legislation specifically applies to child pornography and not to pornography at large. In the Philippines, the enactment of the computer-facilitated child pornography offenses in the Cybercrime Prevention Act is a welcome development – inclusion of these online child pornographic offenses and the associated definitions are based on Title 3 of the Convention on Cybercrime. In Indonesia, the proposals to enact computer-facilitated pornography offenses are considered less comprehensive than the Philippine proposal. It is believed that the Indonesian proposals could benefit from further refinement to get them aligned with the benchmark legislation. Japan has pending computer security legislation; it includes offenses relating to the possession and distribution of obscene electronic records. The Japanese Government plans to amend the Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children. The details of these planned amendments are not available at the date of writing. Way back in 2005, Thailand had considered amendments to its erstwhile online child safety laws, specifically in the area of child pornography. At this point of time, it is not known if or when this legislative proposal will proceed to enactment. As per recommendation of the Indian Standing Committee on IT, the Indian Government has revised the IT Amendment Bill in order to criminalize computer-facilitated dealings with child pornography in accordance with the Convention on Cybercrime. With regard to *online child safety*, the Internet Governance Forum (IGF) is one of the active forums. Table 6.4 shows alignment position of Asia-Pacific countries with regard to Online Child Safety Legislation.

Table 6.4 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to European Cybercrime Convention and ICMEC's Model Child Pornography Legislation

<i>Favorable Alignment</i>	<i>Moderate Alignment</i>	<i>Weak Alignment</i>
Australia	Hong Kong	India*
—	Japan	Indonesia*
—	South Korea	Malaysia
—	Taiwan	New Zealand
—	—	Philippines
—	—	Singapore*
—	—	Thailand
—	—	Vietnam*

*No online child safety laws have been enacted.

Let us consider three important geographies – Asia-Pacific, Europe (where privacy and security laws are very strictly laid out) and the US (where they have chosen a sector-based approach to information security). Positions in these geographies do differ. For example, in the US, there are state laws for prevention of cybercrime. Readers may visit the link given in Ref. #17, Additional Useful Web References, Further Reading which is about US Laws and Legislation. The US Federal Trade Commission estimates that identity theft affects 9 million Americans annually. The US Congress, in September 2008, passed a crack down on cybercrime after adding an amendment containing most of an anti-Spyware bill. This is further discussed in the following section. To conclude the discussion in this section, we note that the world scenario on legal position on cybercrime differs.

6.2.3 Anti-Spam Laws in Canada

In early 2009, the Canadian Government tabled anti-Spam legislation, Bill C-27, The Electronic Commerce Protection Act, to address Spam, counterfeit websites and Spyware. The proposed legislation also brings amendment to Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA – see Box 6.4) which covers online privacy in detail and contains many provisions relevant to E-Mail marketing.

Box 6.4 PIPEDA – The Canadian Act for Protecting Personal Information

Canada has two federal privacy laws, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The *Privacy Act* took effect on 1 July 1983. This Act imposes obligations on some 250 Federal Government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. It gives individuals the right to access and request correction of personal information about themselves held by these Federal Government Organizations.

Individuals are also protected by the PIPEDA that sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. The law gives individuals the right to access and request correction of the personal information these organizations may have collected about them. Initially, PIPEDA applied only to personal information about customers or employees that was collected, used or disclosed in the course of commercial activities by the federally regulated private sector, organizations such as banks, airlines and telecommunications companies. The Act now applies to personal information collected, used or disclosed by the retail sector, publishing companies, the service industry, manufacturers and other provincially regulated organizations. The Act does not apply to the personal information of employees of these provincially regulated organizations.

Basically, PIPEDA is based on the FIPs (Fair Information Practices):

1. Principle 1 – Accountability
2. Principle 2 – Identifying purposes
3. Principle 3 – Consent
4. Principle 4 – Limiting collection
5. Principle 5 – Limiting use, disclosure and retention
6. Principle 6 – Accuracy
7. Principle 7 – Safeguards
8. Principle 8 – Openness
9. Principle 9 – Individual access
10. Principle 10 – Challenging compliance

For more information, contact

The Office of the Privacy Commissioner of Canada

112 Kent Street, Ottawa, ON K1A 1H3

www.priv.gc.ca

1-800-282-1376

Note: The PIPEDA and the FIPs are also addressed in Chapter 29 and Appendix H, respectively, in Nina Godbole (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

There are two laws currently being discussed in Canadian legislative assemblies:

1. **Senate Bill S-220:** The bill was introduced by Senator Yoine Goldstein in early February 2009. It is slated to become the *Anti-Spam Act*. It is a private member's bill with private right of action and criminal remedies. Senator Goldstein has already introduced the Anti-Spam Bill in two previous sessions of parliament. The purpose of this bill is to ban UCE. Bill S-220 replaces the Canadian Bill S-202 (see Ref. #20, Additional Useful Web References, Further Reading). The bill would allow the ISPs to refuse, filter and block Spam E-Mails. The S-220 is proposing to consider Phishing attacks also. According to some legislative experts, there could be potential conflicts between the problematic parts of this proposed legislation and the Canadian Charter of Rights and Freedoms. These conflicts are being looked into because it is felt that it would be a simplified justification for removing sections that contain exemption to spamming (Section 8, subsection 3, paragraphs a, b, c, d and g). The motive for this bill is based on the fact that despite the widespread recognition that Spam is a serious problem which costs our economy billions in fraud and lost productivity, Canada remains the only G8 country without an anti-Spam legislation.
2. **Parliamentary Bill C-27:** The bill was tabled by the government in April 2009, with private right of action, coordination between various enforcement agencies, civil remedies. The Electronic Commerce Protection Act (ECPA) (aka: Bill C-27) is an Anti-Spam Act that covers *E-Mail communications, unauthorized installed applications and the alteration of data during transmission between senders and recipients*. The bill forbids anyone from installing a program on a computer that could send an electronic message without the consent of the owner or user. It also forbids anyone in Canada from sending a commercial message to any electronic address unless the receiver has consented. An exception is if the person sending the message has had a business transaction with the recipient in the previous 18 months. Penalties range from up to \$1 million for individual violators to up to \$10 million for organizations. One of the criticisms against the bill is that "the bill as currently drafted would actually ban the use of the Internet by Canadians unless a person with a website had written consent from a consumer to use it." Instead of demanding consent for certain activities, Ottawa needs to define activity that is bad – for example, creating misleading E-Mail headers.

Box 6.5 ECPA: The New Dawn in Canadian Legislation

The Electronic Commerce Protection Act (ECPA) is a law designed to promote and protect electronic communications while discouraging the abuse of these resources that threaten to impair the reliability, efficiency of electronic activities; prevent additional costs to businesses and consumers; protect the privacy and the security of confidential information and strengthen the confidence of Canadians in the use of electronic means of communication and commercial activities. This enactment also makes several amendments to related laws; the Competition Act, PIPEDA, the Canadian Radiotelevision and Telecommunications Commission Act, and the Telecommunications Act.

The ECPA defines a commercial electronic message as an electronic message that consists of: (a) the content, (b) the hyperlinks and (c) the contact information, where the purpose is to encourage participation in a commercial activity that:

1. Offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
2. offers to provide a business, investment or gaming opportunity;
3. advertises or promotes anything referred to in (1) or (2);
4. promotes a person, including the public image of a person, as being a person who does anything referred to in any of (1)–(3), or who intends to do so.

Box 6.5 ECPA: . . . (Continued)

The ECPA also clearly states that an electronic message which contains a request for consent (i.e., confirmed Opt-In notices) is also considered to be a commercial electronic message. The ECPA also lists several types of excluded communications such as responses to customers' service enquiries and applications, law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defense of Canada and personal communications.

The governance ambit of ECPA looks very large in the sense, which after reading through the act, it looks like every corporation registered under a Federal or Provincial license for the purposes of Commercial Activity is going to be effected by this law. This covers non-profits, co-ops, sole proprietors and partnerships. The Communications Assistance for Law Enforcement Act (CALEA) is the Amendment of ECPA.

Commercial E-Mail can only be sent to a recipient who has consented to receiving it (express or implied – definition below) and the message complies with the purpose of the ECPA described above. All messages being sent must:

1. Clearly identify the person who sent the message and the person (if different) on whose behalf it is sent – *Add your physical postal address and company name to all E-Mails.*
2. Provide a method where the recipient can readily contact the person(s) responsible for sending the message (MUST be active for 60 days after the message was sent) – *Enable replies to go to your customer service and stop using No-Reply.*
3. Provide a working unsubscribe mechanism (more below) that removes an address within 10 days – *The faster the better.*

An important point to note is that the ECPA states that an electronic message is considered to have been sent once its transmission has been initiated (by the sender) and that it is irrelevant if the intended recipient address exists or if message reaches its intended destination. This reference makes bounce management even more important for mailers to monitor and clean from your list. When you are working with your clients/members/subscribers and asking for their consent, there are several things you should remember and incorporate into the process:

1. Clearly state the purpose(s) for which the consent is being sought.
2. Clearly identify the person(s) seeking consent.
3. Clearly define any other prescribed information about how data is collected and plans to be used.

There are significant monetary penalties that have been set out within the Act. The maximum penalty for a violation is \$1,000,000 in the case of an individual, and \$10,000,000 in the case of any other person.

For more details on ECPA refer to the link <http://blog.deliverability.com/2009/04/canadas-electronic-commerce-protection-act.html> (19 August 2009).

6.2.4 Cybercrime and Federal Laws in the US

On 15 September 2008, the US House of Representatives approved the bill H.R. 5938. The amendment, as part of Senate Bill S. 2168, was meant to expand the ability of the Federal Government to prosecute criminal of identity theft and to allow victims to seek compensation for the victims' efforts (time and money) spent on trying to restore their credit. The legislation was signed by President George W. Bush. It had provisions for a fine as well as imprisonment up to 5 years for Spyware. It is believed that this amendment closes the gap on existing identity theft laws which originally only allowed federal prosecution under the scenario that the perpetrator used interstate or foreign communications to access a computer. The only exception were cases involving Federal Government computers or financial institutions. With President's action of signing the bill into Law, Federal prosecutors will be empowered to pursue cases having the perpetrator and victim from the same jurisdiction.

The amendment puts a criminal penalty on the use of malicious Spyware and that of keystroke loggers with the intent of damaging a computer. Furthermore, the amendment eliminates the requirement that the loss must exceed \$5,000, thus, making it a bad behavior to send Spyware that causes any loss. Accused criminals (when proved guilty) will need to pay fine as well as face imprisonment up to 1 year. The legislation would make it an offense to use Spyware or keystroke loggers to damage computers and as such there will be up to 10 years imprisonment. With this bill, it is considered a crime to obtain, delete or release data from a computer or to threaten to crash a computer/computer system. With this bill set, cyberextortion is criminalized by making it a criminal offense to demand money with regard to a protected computer. Those who violate this would end up in prison for a period up to 5 years for the first offense and up to 10 years for the second offense. The bill also adds a conspiracy charge to cybercrime laws and allows confiscation of property/equipment/means used to commit cybercrimes. To understand Computer Crime & Intellectual Property Section of the United States Department of Justice visit [9] in References section.

Box 6.6 The Florida Computer Crimes Act

Unauthorized use of computing facilities is a crime under the Florida Computer Crimes Act. The Act provides definitions to the various terms related to computer crime: *Offenses against intellectual property, offenses against computer equipment or supplies and offenses against computer users.*

The full text of the Florida Computer Crimes Act (1988 version) and a summary of the penalties referenced in the Act are available in the document accessible at the link mentioned at the end of this Box.

The Act specifies the following type of crimes:

1. Offenses against intellectual property;
2. offenses against computer equipment or supplies;
3. offenses against computer users.

- Computer program means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data. It means an internally programmed, automatic device that performs data processing.
- Computer software means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.
- Computer system means a set of related, connected or unconnected computer equipment, devices or computer software.
- Computer network means a set of related, remotely connected devices and communication facilities including more than one computer system with the capability to transmit data among them through communication facilities.
- Computer system services means providing a computer system or computer network to perform useful work.
- Property means anything of value as defined in S.812.011 and includes, but is not limited to, financial instruments, information including electronically produced data and computer software and programs in either machine or human-readable form, and any other tangible or intangible item of value.
- Intellectual property means data, including programs.
- Instrument means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card or marketable security.
- Access means to approach, instruct, communicate with, store data, retrieve data or otherwise make use of any resources of a computer, computer system or computer network.

The Act also defines felony of first, second and third degree. The full text of the Florida Computer Crimes Act (1988 version) and a summary of the penalties as per this Act can be accessed at the following link:
<http://docweb.cns.ufl.edu/docs/d0010/d0010.pdf>

For further details on this act, please refer to the following link:

http://www.clas.ufl.edu/docs/flcrimes/chapter2_1.html (5 December 2009).

6.2.5 The EU Legal Framework for Information Privacy to Prevent Cybercrime

The EU is an economic and political union of 27 member states, located primarily in Europe. Readers can visit the link to understand the EU member countries.^[4] Also see Box 6.7 to know the names of EU member countries. Data protection EU legal framework addressed the principles for information management (fairness, consent, transparency, purpose specification, data retention, security and access). The right to privacy is a highly developed area of law in Europe. All the member states of the EU are also signatories of the European Convention on Human Rights (ECHR). The EU believes that law is the enabler for trust and confidence in the Information Society. However, law is not self-acting; personal data is disclosed by default; online anonymity does not have same status as physical and identification is considered critical for combating crime. However, technology is required to assist in compliance and enforcement. As the global “Information Age” continues to evolve, international understanding of the policy options for data protection also evolves, guided by an understanding of the practical consequences and effectiveness of such laws.

There is a Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) known as the EU directive which regulates the processing of personal data within the EU. It is considered as the most important component of EU privacy and human rights law. In 1995, the European Commission implemented the EU directive.

In the EU, cybercrime law is primarily based on the CoE's Convention on Cybercrime (November 2001). Under the convention, member states are obliged to criminalize:

1. Illegal access to computer system (see Box 6.1);
2. illegal interception of data to a computer system;
3. interfering with computer system without rights and intentional interference with computer data without rights;

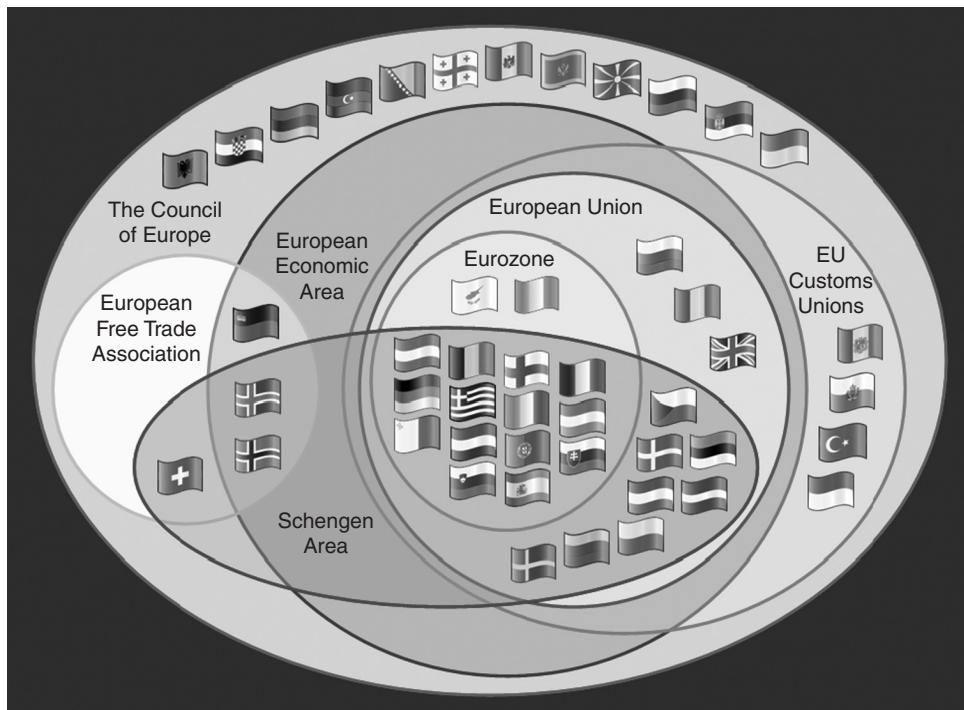
Box 6.7 The EU Member Countries

The European Union (known as the EU) was formed in 1951. At the time of writing this, there are 27 countries that are member of the EU:

1. UK	8. Italy	15. Austria	22. Luxembourg
2. France	9. Netherlands	16. Belgium	23. Estonia
3. Germany	10. Hungary	17. Cyprus	24. Slovakia
4. Denmark	11. Ireland	18. Romania	25. Slovenia
5. Sweden	12. Poland	19. Bulgaria	26. Latvia
6. Finland	13. Portugal	20. The Czech Republic	27. Lithuania
7. Greece	14. Spain	21. Malta	

Bulgaria and Romania are the most recent member states; they joined the EU on 1 January 2007. Other states are also trying to join and negotiations are in progress with them. Figure 6.3 shows the relationships between various supranational European organizations (courtesy Wikipedia). The term *supranational* union implies a supranational political entity that lies somewhere between a “confederation,” that is, an association of states and a federation that is a state.

Note: The mention of CoE is referred to, after Box 6.8, in the context of cybercrime legislation.

Box 6.7 The EU . . . (Continued)**Figure 6.3** Relationships among supranational European organizations.

Note: The color version of the figure is available in CD.

4. the use of inauthentic data with intent to put it across as authentic (data forgery);
5. infringement of copyright-related rights online;
6. interference with data or functioning of computer system;
7. child pornography-related offenses possession/distribution/procuring/producing of child pornographic (recall the discussion in Chapter 1 about COPPA).

Box 6.8 The European Data Protection Directive

Under the EU directive, member states are under obligation to do the following:

1. To ensure that data is processed fairly and lawfully and that it is collected for specified and legitimate purposes and not processed in a manner incompatible with those purposes.
2. The processing of data is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.
3. The data collected is accurate and kept up to date and in a form which permits identification of data subjects.

Box 6.8 The European . . . (Continued)

4. Personal data may be processed only if:
 - The data subject has unambiguously given his consent;
 - processing is necessary for the performance of a contract to which the data subject is party;
 - processing is necessary for compliance with a legal obligation;
 - processing is necessary in order to protect the interests of the data subject;
 - processing is necessary for the performance of a task carried out in the public interest, etc.
5. The directive prohibits the processing of certain personal data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sex life or processing for the purposes of preventive medicine, medical diagnosis, offenses and criminal convictions, etc. except under certain conditions.
6. To provide to the data subject certain information such as identity of the entity processing the data, purposes of the processing, recipients of the data, etc.
7. If the data was not obtained from the data subject, member states are to provide that the entity processing the data must provide the data subject with information such as identity of the entity, purposes of processing, categories and recipients of data, etc.
8. To provide the right to access the data to the data subjects without constraint at reasonable intervals.
9. The data subject must be provided a right to object to the processing of data relating to him and where there is a justified objection, it must be provided that the processing may no longer involve the data.
10. Apart from imposing an obligation to keep the confidentiality of processing of data, the entity processing the data must be required to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure, etc.
11. The transfer of personal data to third countries by member states must be done only under certain conditions.

The Data Protection Directive, therefore, covers a whole range of issues associated with processing of personal data in keeping with the twin objectives of the Directive.

In principle, there are similarities between the US regulation and law enforcement of cybercrime in the EU. Cyberfraud (this term is explained in Chapter 1) and making intentional false representations online (that victims rely on) is a federal offense in the US. Identity theft that takes place in the form of unauthorized use of another person's SSN, driver's license, work ID or credit card online is also a federal cybercrime. ID Theft is addressed in Chapter 5.

6.2.6 Cybercrime Legislation in the African Region

There is a common agreement that the African regions are in dire need for legislation to fight cybercrime. Africa is witnessing explosive growth in ICTs. With this growth, however, cybercrime has also become a reality in this part of the world too. African countries, mostly because of inadequate action and controls to protect computers and networks, are targets of attack. A great deal of criminal activity is said to take place from this part of the world. We heard about the Nigerian 419 scam (more on this is discussed in Section 11.7.19, Chapter 11 in CD) or the story of the young Zambian who hacked into a government website and replaced the picture of the erstwhile president Frederick Chiluba with a cartoon! In early 2008, a good number of South African banks became victims of Phishing attacks (Chapter 5 addresses Phishing attacks).

Box 6.9 The European Convention on Cybercrime

In 1997, there was the meeting of experts and the CoE formed a Committee on Crime in Cyberspace. The experts kept meeting in a clandestine fashion for several years. Ultimately, they succeeded in drafting an international treaty entitled the Convention on Cybercrime known as "the Convention." Finally it was released in June 2001. The Convention on Cybercrime is the first international treaty seeking to address cybercrime and Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was drawn up by the CoE in Strasbourg with the active participation of the CoE's observer states Canada, Japan and the USA. Of the 34 countries that participated in the ceremonial act of signing the Convention in November 2001, only 6 countries have actually ratified the Convention. No major European country has agreed to be bound by the Convention. The only countries that have ratified it are Albania, Croatia, Estonia, Hungary, Lithuania and Romania.

The main aim of the Convention is to pursue "a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international cooperation." The Convention includes a list of crimes that each signatory state must transpose into their own law. It requires the criminalization of such activities as hacking (including the production, sale or distribution of hacking tools) and offenses relating to child pornography, and expands criminal liability for intellectual property violations. It also requires each signatory state to implement certain procedural mechanisms within their laws. For example, law enforcement authorities must be granted the power to compel an ISP to monitor a person's activities online in real time. Finally, the Convention requires signatory states to provide international cooperation to the "widest extent possible" for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. Law enforcement agencies will have to assist police from other participating countries to cooperate with their "mutual assistance requests."

In a significant development of March 2009, the CoE has asked India to be a part of its Convention on Cybercrime. This will lead to efficient cooperation with other 47-member countries, whenever such crimes are committed in India.

Credit card-related frauds are on the rise in the continent, especially in Egypt, South Africa, Kenya, Ghana and Nigeria, with losses estimated in billions of US dollars. E-Mail scams seem to be an African specialty, with West African countries among the major perpetrators. In Section 11.4.2 of Chapter 11, there are several illustrations provided on credit card-related frauds.

Some members of the African Union (Mauritius, South Africa and Zambia) have adopted cybercrime legislation. For example, in Botswana, cybercrime bill passed the second reading in the Parliament in December 2007. The bill is expected to go for third reading in the near future before it is signed into law. A draft Information and Communications Bill 2008 has been introduced in Gambia. The bill includes provisions on computer misuse and cybercrime issues. The East Africa region includes Tanzania, Kenya and Uganda. The progress on cybercrime legislation has been slow in this region, except for Uganda. The Computer Misuse Bill was introduced in 2008 in Uganda and a legislative process has started. The East African countries are trying to coordinate efforts so that the legislations should be similar to the cybercrime laws in the Southern African region. A Cybercrime Bill was prepared in Algeria for submitting it to the Parliament by the end of 2008; this is as per information mentioned on the link http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/features/awi/reportage/2008/05/16/reportage-01. Latest update on the Algerian cybercrime bill position may be found at the link: <http://apex.apkn.org/apex-in-detail/information-society-in-africa/algeria> (28 October 2010).

Overall, it looks like the process of strengthening of legislation has been initiated in a large number of African countries, however, the process is rather slow and sometimes incoherent, and not necessarily taking into account international standards. Although there are exceptions and challenges in the African region, the ability of most African countries to investigate, prosecute and adjudicate cybercrime and cooperate internationally is limited. There is a serious risk that African countries develop legislation that is not compatible or harmonized with that of other countries, in particular that of countries providing servers and services with which cooperation would be most necessary. During the period September 2006–February 2009, Economic Crime Division of the Directorate General of Human Rights and Legal Affairs took up a cybercrime project. At the end of that project, they submitted their final report according to which the legislative scenario in some of the African countries emerges to be as presented in Table 6.5.

Table 6.5 | Cybercrime legislation in some of the African countries

Name of the African Countries	Recommendation on Cybercrime Legislation
Nigeria	There are several acts in force. They cover several aspects of cybercrime. A draft law on cybercrime is before the Parliament. The draft was expecting CoE review to elicit their support to bring it fully in line with the Convention. An analysis of the draft has been provided by the CoE in January 2008.
Ghana	A draft bill on cybercrime is available but needs a review to validate against the provision of the Convention. Accession to the Convention should be considered in the future.
Togo	There is no specific legislation in place. A working group needs to be established to develop a law on cybercrime in line with the Convention.
Niger	There is a package of laws prepared to provide a legal framework for information and communication technologies. The package has been submitted and is before the Parliament. This package expects deep analysis by the CoE. Accession to the Convention on cybercrime should also be considered.
Mali	Currently, no legislation is available. A national law on cybercrime is expected to be developed along the lines of international standards such as the Convention on Cybercrime.
Benin	Draft amendments to the criminal code and criminal procedure code are presented to the Parliament. It is recommended that relevant provisions should be reviewed to take into account the Convention on Cybercrime's views.
Congo	Currently, no legislation is available; however, review of criminal code and criminal procedure code is underway. It was recommended that a working group be established to develop a specific law on cybercrime in line with the Convention with the support of the CoE. Accession to the Convention should be considered once the law is in place.

Source: The Report by the Economic Crime Division of the Directorate General of Human Rights and Legal Affairs, Cybercrime project run during the period September 2006–February 2009).

Note: For CoE Convention on Cybercrime frequently asked questions and answers, visit the link at <http://www.cybercrime.gov/COEFAQs.htm> (24 August 2009). To get an idea about the location of the countries in the African continent given in the table, readers can consult the country-wise map of Africa. One such map can be accessed at the following URL: <http://www.africaguide.com/afmap.htm>

In South Africa “peace and security” is recognized as the essential human right. South Africa acknowledges peace and security to be fundamental and intrinsic to the democratic right for its citizens. South Africa being one of the most developed and prosperous economies in the African region, we must understand the legislative position of South Africa about cyberlaws. The discussion in this subsection is with that intent. During 13 November 2008 speech in Geneva at the high-level segment of the ITU Council, Radhakrishna L Padayachie, Deputy Minister of Communications, Republic of South Africa, addressed two issues related to the building of confidence and security in the use of ICTs, namely,

1. The measures that are in place and planned by the Republic of South Africa to enhance cooperation and collaboration on cybersecurity with other stakeholders at the regional, national and global levels and
2. the main challenges that should be tackled to ensure that the information society is safer and more secure at the global level.

In general, however, South African law does not prohibit unwelcome advertising. Advertising by the marketing communications industry is regulated by the Advertising Standards Authority of South Africa. In addition to this, South Africa has also got legislation governing “Spam.” In July 2009, South African President assented to the *Electronic Communications and Transactions Act* (ECT Act) 2002. The purpose of the ECT Act is

“to provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-Strategy for the Republic; to promote universal access to electronic transactions; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of E-government services; and to provide for matters connected therewith.”

The material in this Act is divided into 14 chapters – among them are Chapter 7 is about Consumer Protection, Chapter 8 is about Protection of Personal Information and Chapter 13 is about Cybercrime.

In South Africa, the Department of Communications is mandated by the Electronic Communications and Transaction Act 2002, among others, to deal with cybercrime and other cybersecurity-related issues:

1. As far as identity management is concerned, the South African Accreditation Authority (SAAA) is responsible for accreditation of authentication services and products and more importantly the accreditation of service providers who will issue advanced digital signatures. This is for the purposes of ensuring business efficiency, quality of services, information security, and privacy and consumer trust in online transactions.
2. For cryptography, South African legislation provides for the registration of the cryptograph service providers with the Department of Communications.
3. South African legislation has the provision for the establishment of a cyberinspectorate, among others, to ensure compliance of cryptography service providers, authentication service providers and critical database management.

In line with the key cybersecurity focus areas developed by the GCA (*Global Cybersecurity Agenda* of the ITU – International Telecommunication Union), the planned framework in South Africa will, among others, encompass the following key features:

1. **Legal measures:** In view of the borderless nature of cyberspace, our national laws that currently address the threat of cybercrime may have to be evaluated against the international best practices envisaged

in the model cybercrime legislation that is recommended as globally applicable and interoperable. This work will necessitate reviewing our existing national laws that deal with cybercrimes.

2. **Technical and procedural measures:** The emphasis will be on providing key measures to promote the adoption of enhanced approaches to improve security and risk management in cyberspace. The Republic of South Africa is working toward establishing Computer Security Incident Response Teams (CSIRTs) under the auspices of the Electronic Communication Security (Pty) Ltd (COMSEC). South Africa is also collaborating with some countries with a view to become a member of the Forum for Incident Response and Security Teams (FIRSTs).

As part of South Africa's determination to collaborate on cybersecurity with other stakeholders at the regional, national and global levels, South Africa has joined the Southern Africa Development Community (SADC) that consists of 14 African countries. SADC countries are on track to harmonize their Internet laws to effectively deal with computer-related crimes, and have finalized legislation for fighting cybercrime. It is said that all the SADC countries have agreed to alter parts of their cybercrime laws and come up with common rules.

For greater details about what the ECT Act of South Africa states about Spam filters, readers are advised to visit Ref. #23, Additional Useful Web References, Further Reading. Having taken an overview of the world legislative picture, now we come to India-specific discussion with focus on the IT Act and its amendments.

6.3 Why Do We Need Cyberlaws: The Indian Context

Cyberlaw is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks. Under the purview of cyberlaw, there are several aspects, such as, *intellectual property, data protection and privacy, freedom of expression and crimes committed using computers*. The Indian Parliament passed its first cyberlaw, the ITA 2000, aimed at providing the legal infrastructure for E-Commerce in India. ITA 2000 received the assent of the President of India and it has now become the law of the land in India. The Government of India felt the need to enact relevant cyberlaws to regulate Internet-based computer-related transactions in India. It manages all aspects, issues, legal consequences and conflict in the world of cyberspace, Internet or WWW. In the Preamble to the Indian ITA 2000, it is mentioned that it is an act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*. The reasons for enactment of cyberlaws in India are summarized below:

1. Although India possesses a very well-defined legal system, covering all possible situations and cases that have occurred or might take place in future, the country lacks in many aspects when it comes to newly developed Internet technology. It is essential to address this gap through a suitable law given the increasing use of Internet and other computer technologies in India.
2. There is a need to have some legal recognition to the Internet as it is one of the most dominating sources of carrying out business in today's world.
3. With the growth of the Internet, a new concept called *cyberterrorism* came into existence. Cyberterrorism includes the use of disruptive activities with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives in the world of cyberspace. It actually is about committing an old offense but in an innovative way.

Keeping all these factors into consideration, Indian Parliament passed the Information Technology Bill on 17 May 2000, known as the ITA 2000. This law is based on Model UNCITRAL law for E-Commerce (see Ref. #11, Articles and Research Papers, Further Reading). It talks about cyberlaws and forms the legal framework for electronic records and other activities done by electronic means. There are strengths as well as limitations in the ITA 2000; they are explained in Sections 6.4.2 and 6.4.3. A legal framework for the cyberworld was conceived in India, in the form of a draft E-Commerce Act 1998 – thereafter, the subject of cyberlaws started haunting the government. The basic law for the cyberspace transactions in India has emerged in the form of the ITA 2000. With that background, the Indian IT Act is briefly discussed in the following section.

6.4 The Indian IT Act

As mentioned above, this Act was published in the year 2000 with the purpose of providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*. Electronic communications involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies. Another purpose of the Indian IT Act was to amend the Indian Penal Code (IPC),^[11] the Indian Evidence Act 1872,^[12] the Bankers' Books Evidence Act 1891,^[13] the Reserve Bank of India Act 1934^[14] and matters connected therewith or incidental thereto. Cybercrimes punishable under various Indian laws are mentioned in Box 6.10. The Reserve Bank of India Act has got Section 58B about Penalties. Subsequently, the Indian IT Act underwent some important changes to accommodate the current cybercrime scenario; a summary of those changes is presented in Table 6.7 – note specially the changes to Section 66 and the corresponding punishments for cyberoffenses. Readers should also refer to Section 6.8.1 (Overview of Changes Made to the Indian IT Act) where the changes are explained in details.

Box 6.10

Cybercrimes and Other Related Crimes Punishable under Indian Laws

1. Under Section 65 of Indian Copyright Act any person who knowingly makes, or has in his/her possession, any plate for the purpose of making infringing copies of any work in which Copyright subsists is punishable with imprisonment which may extend to 2 years with fine.
2. Sending pornographic or obscene E-Mails are punishable under Section 67 of the IT Act.
 - An offense under this section is punishable on first conviction with imprisonment for a term, which may extend to 5 years and with fine, which may extend to 1 lakh rupees (₹ 100,000).
 - In the event of a second or subsequent conviction, the recommended punishment is imprisonment for a term, which may extend to 10 years and also with fine which may extend to 2 lakh rupees (₹ 2,00,000).
3. E-Mails that are defamatory in nature are punishable under Section 500 of the Indian Penal Code (IPC) that recommends an imprisonment of upto 2 years or a fine or both.
4. Threatening E-Mails are punishable under the provisions of the IPC pertaining to criminal intimidation, insult and annoyance (CHAPTER XXII) and extortion (CHAPTER XVII).
5. E-Mail spoofing is covered under provisions of the IPC with regard to fraud, cheating by personation (CHAPTER XVII) and forgery (CHAPTER XVIII).

The scope and coverage of the Indian IT Act is briefly described in Section 27.4, Ref. #6, Books, Further Reading. The structure of the Indian ITA 2000 is provided in Table 6.6 for readers' immediate reference. The sections mentioned in bold italics are relevant in the discussion of cybercrime and information security.

Table 6.6 | The Indian ITA 2000: Summary of contents (main elements only)

<i>Chapter Number</i>	<i>Chapter Title</i>	<i>Names of the Sections in the Chapter</i>
CHAPTER I	<i>Preliminary</i>	1. Short title, extent, commencement and applications 2. Definitions of key terms mentioned in the Act 3. Authentication of electronic records
CHAPTER II	<i>Digital Signature and Electronic Signature</i>	
CHAPTER III	<i>Electronic Governance</i>	4. Legal recognition of electronic records 5. Legal recognition of electronic signatures 6. Use of electronic records and digital signatures in government and its agencies 7. Retention of electronic records 8. Publication of rule, regulation, etc., in Electronic Gazette 9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in an electronic form 10. Power to make rules by Central Government in respect of digital signature
CHAPTER IV	<i>Attribution, Acknowledgment and Despatch of Electronic Records</i>	11. Attribution of electronic records 12. Acknowledgment of receipt 13. Time and place of dispatch and receipt of electronic record
CHAPTER V	<i>Secure Electronic Records and Secure Electronic Signature</i>	14. Secure electronic record 15. Secure digital signature 16. Security procedures and practices 17. Appointment of Controller and other officers 18. Functions of Controller 19. Recognition of foreign Certifying Authorities 20. Controller to act as repository 21. License to issue Digital Signature Certificates 22. Application for license 23. Renewal of license 24. Procedure for grant or rejection of license 25. Suspension of license 26. Notice of suspension or revocation of license 27. Power to delegate 28. Power to investigate contraventions 29. <i>Access to computers and data</i>
CHAPTER VI	<i>Regulation of Certifying Authorities</i>	30. Certifying Authority to follow certain procedures 31. Certifying Authority to ensure compliance of the Act, etc. 32. Display of license 33. Surrender of license 34. Disclosure

(Continued)

Table 6.6 | (Continued)

<i>Chapter Number</i>	<i>Chapter Title</i>	<i>Names of the Sections in the Chapter</i>
CHAPTER VII	<i>Electronic Signature Certificates</i>	35. <i>Certifying Authority to issue Digital Signature Certificate</i> 36. Representations upon issuance of Digital Signature Certificate 37. Suspension of Digital Signature Certificate 38. Revocation of Digital Signature Certificate 39. Notice of suspension or revocation
CHAPTER VIII	<i>Duties of Subscribers</i>	40. Generating key pair 41. Acceptance of Digital Signature Certificate 42. Control of private key
CHAPTER IX	<i>Penalties, Compensation and Adjudication</i>	43. Penalty for damage to computer, computer system, etc. 44. Penalty for failure to furnish information return, etc. 45. Residuary penalty 46. Power to adjudicate 47. Factors to be taken into account by the adjudicating officer
CHAPTER X	<i>The Cyber Regulations Appellate Tribunal</i>	48. Establishment of Cyber Appellate Tribunal 49. Composition of Cyber Appellate Tribunal 50. Qualifications for appointment 51. Term of office, conditions of services, etc. 52. Salary, allowances and other terms and conditions of service of Presiding Officer 53. Filling up of vacancies 54. Resignation and removal 55. Orders constituting Appellate Tribunal 56. Staff of the Cyber Appellate Tribunal 57. Appeal to Cyber Appellate Tribunal 58. Procedure and powers of the Cyber Appellate Tribunal 59. Right to legal representation 60. Limitation 61. Civil Court not to have jurisdiction 62. Appeal to High Court 63. Compounding of contraventions 64. Recovery of penalty or compensation
CHAPTER XI	<i>Offences</i>	65. <i>Tampering with computer source documents</i> 66. <i>Computer-related offences</i> 67. Punishment for publishing, transmitting obscene material in electronic form
	<i>66A. Punishment for offensive messages</i>	
	<i>66B. Punishment for dishonestly receiving stolen computers, etc.</i>	

(Continued)

Table 6.6 | (Continued)

<i>Chapter Number</i>	<i>Chapter Title</i>	<i>Names of the Sections in the Chapter</i>
	66C. <i>Punishment for ID theft</i> 66D. <i>Punishment for cheating by personation with use of computers</i> 66E. <i>Punishment for privacy violation</i> 66F. <i>Punishment for cyber terrorism</i>	68. Power of Controller to give directions 69. Power to issue directions for inception or monitoring or decryption of information 70. Protected system 71. <i>Penalty for misrepresentation</i> 72. <i>Penalty for breach of confidentiality and privacy</i> 73. <i>Penalty for publishing Digital Signature Certificate false in certain particulars</i> 74. <i>Publication for fraudulent purpose</i> 75. Act to apply for offence or contravention committed outside India 76. Confiscation 77. Compensation, penalties or confiscation not to interfere with other punishments 78. Power to investigate offences 79. Exemption from liability of intermediary in certain cases 80. Power of police officer and other officers to enter, search, etc. 81. Act to have overriding effect 82. Chairperson, Members, officers and employees to be public servants 83. Power to give directions 84. Protection of action taken in good faith 85. Offences by companies 86. Removal of difficulties 87. Power of Central Government to make rules 88. Constitution of Advisory Committee 89. Power of Controller to make regulations 90. Power of State Government to make rules
CHAPTER XII	<i>Intermediaries not to be Liable in certain Cases</i>	
CHAPTER XIII	<i>Miscellaneous</i>	

Note: Digital signature and cryptography concepts, use of symmetric and asymmetric keys, etc. related concepts are explained in Ref. #7, Books, Further Reading. Readers must refer to the paper copy of the IT Act.

From Table 6.6, we can see that in particular, Sections 65, 66, 67, 71, 72, 73 and 74 in CHAPTER XI (Offences) of the Indian ITA 2000 are relevant to the discussion of cybercrime in legal context. The relevant portion from that is as follows:

1. Section 65: Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer

programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to 3 years, or with fine which may extend up to 2 lakh rupees (₹ 2,00,000), or with both.

Explanation: For the purposes of this section, “computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

2. Section 66: Computer-related offences

- (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
- (2) Whoever commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to 5 lakh rupees (₹ 5,00,000), or with both.

3. Section 67: Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to 3 years and with fine which may extend to 5 lakh rupees (₹ 5,00,000) and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to 5 years and also with fine which may extend to 10 lakh rupees (₹ 10,00,000).

4. Section 71: Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

5. Section 72: Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there-under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

6. Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars

- (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that:
 - (a) The Certifying Authority listed in the certificate has not issued it; or
 - (b) the subscriber listed in the certificate has not accepted it; or
 - (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
- (2) Any person who contravenes the provisions of subsection (1) shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

7. Section 74: Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

Table 6.7 presents the brief overview of the significant changes brought out by the IT Amendment Bill 2008. Also refer to Section 6.8.1 (Overview of Changes Made to the Indian IT Act) in which changes are explained in great detail.

Box 6.11 Data Protection and the New Clause 43A under the Amended IT Act

The amended Indian IT Act provides for penalty for damage to computers, computer systems under the title *Penalty and Adjudication* in Section 43 that is widely interpreted as a clause to provide data protection in the country. Unauthorized access to a computer, computer system or computer network is punishable with a compensation of up to 1 crore rupees (₹ 1,00,00,000). This section has been improved to include stealing of computer source code for which compensation can be claimed. (Computer source has been defined.) Data protection has now been made more explicit through insertion of a new Clause 43A that provides for compensation to an aggrieved person whose personal data including sensitive personal data may be compromised by a company, during the time it was under processing with the company, for failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices.

Furthermore, reasonable security practices and procedures will constitute those practices and procedures that protect such information from unauthorized access, damage, use, modification, disclosure or impairment as may be specified in an agreement between the parties or as may be specified in any law in force. In the absence of such an agreement or any law, the Central Government will prescribe security practices and procedures in consultation with professional bodies or associations:

(a) This explanation gives scope for recognition of security professional bodies such as Data Security Council of India (DSCI), which is an industry initiative promoted by NASSCOM. The best practices and standards for security that DSCI may prescribe to the IT and BPO companies may be accepted by the government. Regulation of companies for compliance with such standards and practices can fall within the ambit of DSCI.

(b) Sensitive personal information may be prescribed by the Central Government in consultation with professional bodies or associations. In the context of outsourcing to India, this can be defined to be in line with compliance requirements of the EU (European Union) Data Protection Directive and US laws such as Health Insurance Portability and Accountability Act (HIPAA) or Graham-Leach-Bliley Act (GLBA).

Penalty for breach of confidentiality and privacy: Under Section 72, it is presently restricted to those who gain access to an electronic record or document under the powers conferred under this Act. A new Section 72A has been added that provides punishment for disclosure of information in breach of a lawful contract. Any person including an intermediary who has access to any material containing personal information about another person, as part of a lawful contract, discloses it without the consent of the subject person will constitute a breach and attract punishment with imprisonment of up to 3 years and/or a fine of 5 lakh rupees (₹ 5,00,000). This is a strong deterrent, and also will bring those responsible for breaching data confidentiality, under lawful contracts, to justice. Along with Section 43A, Section 72A strengthens the data protection regime in the country. It will go a long way in promoting trust in transborder data-flows to India.

Note: This information is as per the NASSCOM Whitepaper "Data Protection and Cyber Crime under amended IT Act." The whitepaper was released by DSCI in December 2008. Data Security Council of India (DSCI) is an initiative under NASSCOM.

Table 6.7 | Summary of changes to the Indian IT Act (significant changes brought out by the IT Amendment Bill 2008)

<i>Section No.</i>	<i>Changes Made</i>
1	Section 1(4) list of excluded documents removed. To be notified through Gazette.
2	Section 2(d) modified, and the term “Digital Signature” replaced with “Electronic Signature” in the Act. Section 2(ha) added to define “Communication Device” which will include mobile phones, ATM, PDAs, etc. Section 2(j) “Computer Systems” and “Communication Devices” and “Wire” and “Wireless” added. Section 2(k) “Communication Device” added. Section 2(na) introduced to define the term “Cyber Cafe.” Section 2(nb) introduced to define the term “Cyber Security.” Section 2(ta) and Section 2(tb) introduces the term of “Electronic Signature” and “Electronic Signature Certificate.” Section 2(ua) defines “Indian Computer Emergency Response Team.” Section 2(v) “Message” included in the definition of “Information.” Section 2(w) “Intermediary” defined. It includes telecom. <i>Note:</i> Service providers, network service providers, Internet service providers, webhosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.
3	Section 3 now refers to legal recognition of electronic documents. New Section 3A introduced to define Electronic Signature.
4 and 5	No significant change.
6	New Section 6A introduced to provide for appointment of service providers in E-Governance services and enable delivery of services by private service providers.
7	New Section 7A introduced to make audit of electronic documents mandatory wherever the legally physical records were subject to audit.
8 and 9	No change.
10	No significant change. New Section 10A specifies that contract formation is possible with offer and acceptance being in electronic form.
11, 12, 13 and 14	No significant change.
15 and 16	Defines “Secured Electronic Signature” and redefines “Security Procedure.”
17, 18, 19	No significant change.
20	Section omitted.
21	No significant change.
22 and 23	The amount of specified upper limit on the fees omitted.
24, 25, 26, 27	No significant change.
28 and 29	The powers of Controller have been restricted to contraventions under chapter VI.
30	Consequential Changes with introduction of Electronic Signatures.
31, 32, 33, 34	No significant change.
35	Subsection 35(4) modified.
36	Additional points to be added in the certificate indicated.

(Continued)

Table 6.7 | (Continued)

<i>Section No.</i>	<i>Changes Made</i>
37, 38, 39	No change.
40	No change in Section 40 but a new section added as mentioned below. New Section 40A specifies the duties of the subscriber of Electronic Signatures Certificate.
41 and 42	No change.
43	Two new contraventions added – Contraventions corresponding to earlier Section 65 and Section 66 added for civil liability. Compensation limit removed. New Section 43A included for “Data Protection” need specifies liability for a body corporate handling sensitive data, introduces concept of “reasonable security practices” and sensitive personal data. No limit for compensation.
44 and 45	No significant change.
46	The powers of the Adjudicator limited for claims upto ₹ 5 crore (₹ 5,00,00,000). Civil Court’s authority introduced for claims beyond ₹ 5 crore (₹ 5,00,00,000).
47	No significant change.
48	Changes name of Cyber Regulations Appellate Tribunal to Cyber Appellate Tribunal.
49	Cyber Appellate Tribunal (CAT) is made a multimember entity. Provision for benches introduced, non-judicial members can be members of the Tribunal.
50	Specifies qualifications for appointment of Chairperson and Members of the CAT.
51 and 52	Specifies terms and other conditions of appointment of Chairman and Members of CAT (Cyber Appellate Tribunal). New Sections 52A, B, C and D introduced defining powers of the Chairperson of CAT for conduct of business.
53, 54, 55, 56	No significant change.
57, 58, 59, 60	No change.
61	Amended to accommodate jurisdiction of Civil Courts for disputes involving claims of over ₹ 5 crore (₹ 5,00,00,000).
62 and 63	No change.
64	No significant change.
65	No change.
66	<i>Note:</i> This is a notable feature of the changes made – note the “punishments.” The clause has been rewritten with significant changes. Applies to all contraventions listed in Section 43 and shall be punishable with imprisonment for a term which may extend to three(3) years or with fine which may extent up to ₹ 5 lakhs (₹ 5,00,000) and both. The section applies if act is done “dishonestly” or “fraudulently” as defined in CrPC (Criminal Procedure Code). New Sections added under 66A, 66B, 66C, 66D, 66E and 66F to cover new offences. Section 66A: Sending offensive messages. Punishment: Imprisonment for a term which may extend to three years and fine. Section 66B: Receiving a Stolen Computer Resource Punishment: Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh (₹ 1,00,000) or with both.

(Continued)

Table 6.7 | (Continued)

<i>Section No.</i>	<i>Changes Made</i>
	<p>Section 66C: Identity Theft Punishment: Imprisonment for a term which may extend to three years also be liable to fine which may extend to rupees one lakh (₹ 1,00,000).</p>
	<p>Section 66D: Cheating by personation Punishment: Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees (₹ 1,00,000).</p>
	<p>Section 66E: Violation of Privacy Punishment: Imprisonment for a term which may extend to three years or with fine not exceeding two lakh rupees (₹ 2,00,000) or with both.</p>
	<p>Section 66F: Cyber Terrorism Punishment: Imprisonment which may extend to imprisonment for life. 67 Fine increased to ₹ 5 lakhs (₹ 5,00,000) for first instance and ₹ 10 lakhs (₹ 10,00,000) for subsequent instance. Imprisonment reduced to three years for first instance and 5 years for subsequent instance. New Section 67A introduced to cover material containing “sexually explicit act.” Punishment: On first conviction with imprisonment for a term which may extend to five years and with fine which may extent to 10 lakhs (₹ 10,00,000). In the event of second and subsequent conviction with imprisonment for a term which may extend to seven years and also with fine which may extent to 10 lakhs (₹ 10,00,000). New Section 67B introduced to cover child explicit act or conduct. Punishment: On first conviction with imprisonment for a term which may extend to five years and with fine which may extent to 10 lakhs (₹ 10,00,000). In the event of second and subsequent conviction with imprisonment for a term which may extend to seven years and also with fine which may extent to 10 lakhs (₹ 10,00,000). New Section 67C: This provision will require Intermediaries to preserve and retain certain records for a stated period. Punishment: Imprisonment for a term which may extend to three years and also be liable to pay fine.</p>
68	Refers to the powers of the Controller to direct Certifying Authorities for compliance. No significant change. Penal powers to be applicable only on intentional violation.
69	Scope extended from decryption to interception, monitoring also. Power lies with the authorized government agency of the Central Government. New Section 69A: Introduced to enable blocking of websites. If an Intermediary is not cooperative. Punishment: Imprisonment for a term which may extent to seven years and also be liable to fine. New section 69B: Provides powers for monitoring and collecting traffic data, etc. If an Intermediary is not cooperative.
70	Punishment: Imprisonment for a term which may extent to three years and also be liable to fine. Critical Infrastructure System defined and section restricted to only such systems. Security practices to be notified.
70B	New Section 70A: Added to define National Nodal Agency for Critical Information Infrastructure Protection. Indian Computer Emergency Response Team (Cert India) appointed as the Nodal agency for incident response.
71 and 72	No change. New Section 72A: Introduced for punishment for disclosure of information in breach of lawful Contract (data protection purpose).

(Continued)

Table 6.7 | (Continued)

Section No.	Changes Made
73, 74, 75, 76	No change.
77	No significant change. New Section 77A: Introduced to provide for Compounding of offences other than offences for which imprisonment for life or imprisonment for a term exceeding three years has been provided. New Section 77B: Introduced to consider all offences punishable with imprisonment of three years and above under the Act as Cognizable offence and offence punishable with imprisonment for 3 years as bailable.
78	Power to investigate any cognizable offence vested with Inspectors instead of DSPs (Deputy Superintendent of Police). <i>Note:</i> This is notable change of bringing down the investigation authority lower in the hierarchy.
79	Exemption from liability of intermediary in certain cases – some exceptions have been added – no liability if intermediary provides only Internet access, observed due diligence, had no actual knowledge of offence, etc. New Section 79 A: Introduced to provide for the government to designate any government body as an Examiner of Electronic Evidence.
80	The powers, earlier available to DSPs, is now made available to Inspectors. <i>Note:</i> This is notable change of bringing down the investigation authority lower in the hierarchy.
81	Amended to keep the Copyright and Patent Acts fully applicable.
81A	No change.
82	No significant change.
83 and 84	No change. Section 84A: New section introduced to enable the government to prescribe encryption methods. New Section 84B: Introduced to make “abetment” punishable as the offence itself is under the IT Act 2000. New Section 84C: Introduced to make an “attempt to commit an offence” punishable with half of the punishment meant for the offence.
85 and 86	No change.
87	Consequential changes made.
88 and 89	No change.
90	No significant change.
91–94	Omitted

Box 6.12 Digital Evidence and its Admissibility in Courts

Digital/electronic evidence is probative information stored in digital form that a party may use at trial. It includes computer printouts, E-Mails, digital photographs, ATM transaction logs, spreadsheets and others. With increased computerization and technology as well as the rise of the digital office, courts have been forced to allow for the admittance of digital evidence. In the Indian ITA 2000, the word Evidence appears in Section 58 (Procedure and Powers of the Cyber Appellate Tribunal), The Second Schedule, Clause 65B (Admissibility of Electronic Records). It is said that the enactment and adoption of the Indian Evidence Act was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of evidences in the Indian Courts of Law.

Box 6.12 Digital Evidence and . . . (Continued)

There are challenges in digital evidence handling. Today, the computer technology is very complex, although the usability for the end-users is very high. The extensive amount of data stored on today's computers and the limited resources available to analyze computer evidence are two of the facts that contribute to delays in the return of digital evidence. With the worldwide reach of the Internet, crimes are no longer easily defined as occurring within a particular city, state or even within the country. More and more criminals are coming from around the world and committing crimes against their targeted victims via the Internet. In such situations, law enforcement officials may find it difficult to obtain evidence and even impossible to enforce warrants for searches and seizures of digital evidence stored abroad. The complexity of most types of digital evidence, as well as the methods in which law enforcement comes into control of the evidence, can raise issues of admissibility, that is, admissibility of digital evidence. Courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available. More about digital evidence is addressed in Chapters 7 and 8.

6.4.1 Admissibility of Electronic Records: Amendments made in the Indian ITA 2000

The Second, the Third and the Fourth Schedule of the Indian ITA 2000 indicates how the three acts, namely, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and The Reserve Bank of India Act 1934 have been amended. In this section, these amendments are presented. This is particularly important for the discussion about forensics in Chapter 7. It appears that the maximum amendments have been made to the Indian Evidence Act.

In the Indian Evidence Act, CHAPTER IV is about Oral Evidence and CHAPTER V is about Documentary Evidence. In the Indian IT Act, the Second Schedule presents "Amendments to the Indian Evidence Act of 1872." The text from there pertaining to the amendment is presented below.

The Second Schedule of the Indian ITA 2000: Amendment to the Indian Evidence Act

1. In Section 3:
 - (a) In the definition of "Evidence," for the words "all documents produced for the inspection of the Court," the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;
 - (b) after the definition of "India," the following shall be inserted, namely, the expressions "Certifying Authority," "digital signature," "Digital Signature Certificate," "electronic form," "electronic records," "information," "secure electronic record," "secure digital signature" and "subscriber" shall have the meanings, respectively, assigned to them in the Information Technology Act 2000.
2. In Section 17, for the words "oral or documentary," the words "oral or documentary or contained in electronic form" shall be substituted.
3. After Section 22, the following section shall be inserted, namely, when oral admission as to contents of electronic records is relevant.

"22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."
4. In Section 34, for the words "Entries in the books of account," the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In Section 35, for the word "record," in both the places where it occurs, the words "record or an electronic record" shall be substituted.
6. For Section 39, the following section shall be substituted, namely, *What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.*

"39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made."

7. After Section 47, the following section shall be inserted, namely, *Opinion as to digital signature where relevant.*

"47A. When the Court has to form, an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. In Section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.
9. After Section 65, the following sections shall be inserted, namely, *Special provisions as to evidence relating to electronic record.*

"65A. The contents of electronic records may be proved in accordance with the provisions of Section 65B."

Admissibility of Electronic Records

- 65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.
- (2) The conditions referred to in subsection (1) in respect of a computer output shall be the following, namely,
- (a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
 - (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
 - (c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents and
 - (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in Clause (a) of subsection (2) was regularly performed by computers, whether:
 - (a) By a combination of computers operating over that period; or
 - (b) by different computers operating in succession over that period; or
 - (c) by different combinations of computers operating in succession over that period; or
 - (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.
- (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say:
 - (a) Identifying the electronic record containing the statement and describing the manner in which it was produced;
 - (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
 - (c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
- (5) For the purposes of this section:
 - (a) Information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
 - (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
 - (c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation: For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there-from by calculation, comparison or any other process.

10. After Section 67, the following section shall be inserted, namely, *Proof as to digital signature*.

“67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.”

11. After Section 73, the following section shall be inserted, namely, *proof as to verification of digital signature*.

“73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct:

- (a) That person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
- (b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.”

Explanation: For the purposes of this section, “Controller” means the Controller appointed under subsection (1) of Section 17 of the Information Technology Act 2000.

12. Presumption as to Gazettes in electronic forms

After Section 81, the following section shall be inserted, namely,

“81A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.”

13. Presumption as to electronic agreements

After Section 85, the following sections shall be inserted, namely,

“85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.”

14. Presumption as to electronic records and digital signatures

85B (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that:

- (a) The secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;
- (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

15. Presumption as to Digital Signature Certificates

85C The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

16. Presumption as to electronic messages

After Section 88, the following section shall be inserted, namely,

“88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.”

Explanation: For the purposes of this section, the expressions “addressee” and “originator” shall have the same meanings, respectively, assigned to them in Clauses (b) and of subsection (1) of Section 2 of the Information Technology Act 2000.

17. Presumption as to electronic records of five years old

After Section 90, the following section shall be inserted, namely,

“90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that

the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf.”

Explanation: Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This explanation applies also to Section 81A.

For Section 131, the following section shall be substituted, namely, production of documents or electronic records which another person, having possession, could refuse to produce.

131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.

The Third Schedule of the Indian IT Act 2000: Amendment to the Bankers' Books Evidence Act

1. In Section 2:
 - (a) For Clause (3), the following clause shall be substituted, namely, '(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;
 - (b) for Clause (8), the following clause shall be substituted, namely, '(8) "certified copy" means when the books of a bank:
 - (A) Are maintained in written form, a copy of any entry in such books together with a certificate written; the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and
 - (B) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of Section 2A.
2. After Section 2, the following section shall be inserted, namely, *Conditions in the printout*.

"2A. A printout of entry or a copy of printout referred to in subsection (8) of Section 2 shall be accompanied by the following, namely,

 - (a) A certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager and
 - (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of:
 - (A) The safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons;
 - (B) the safeguards adopted to prevent and detect unauthorized change of data;
 - (C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

- (D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
 - (E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;
 - (F) the mode of identification of such data storage devices;
 - (G) the arrangements for the storage and custody of such storage devices;
 - (H) the safeguards to prevent and detect any tampering with the system and
 - (I) any other factor which will vouch for the integrity and accuracy of the system.
- (c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data."

The Fourth Schedule of the Indian IT Act 2000: Amendment to the Reserve Bank of India Act

In the Reserve Bank of India Act 1934, in Section 58, in subsection (2), after Clause (p), the following clause shall be inserted, namely,

"the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in Clause (c) of Section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers."

6.4.2 Positive Aspects of the ITA 2000

The Indian ITA 2000, though heavily criticized for not being specific on cybercrimes, in our opinion, does have a few good points. At the same time, there is, also, fair amount of vagueness in the Act. This is briefly discussed here in this section.

1. Prior to the enactment of the ITA 2000 even an E-Mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the ITA 2000 changed this scenario by legal recognition of the electronic format. Indeed, the ITA 2000 is a step forward.
2. From the perspective of the corporate sector, companies are able to carry out E-Commerce using the legal infrastructure provided by the ITA 2000. Till the coming into effect of the Indian cyberlaw, the growth of E-Commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.
3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the ITA 2000.
4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a backup. Under the ITA 2000, it became possible for corporate to have a statutory remedy if anyone breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the ITA 2000 is in the form of monetary damages, by the way of compensation, not exceeding ₹ 10,000,000.
5. ITA 2000 defined various cybercrimes. Prior to the coming into effect of the Indian Cyberlaw, the corporate were helpless as there was no legal redress for such issues. However, with the ITA 2000 instituted, the scenario changed altogether.

6.4.3 Weak Areas of the ITA 2000

As mentioned before, there are limitations too in the IT Act; those are mainly due to the following gray areas:

1. The ITA 2000 is likely to cause a conflict of jurisdiction.
2. E-Commerce is based on the system of domain names. The ITA 2000 does not even touch the issues relating to domain names. Domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law. The law does not address the rights and liabilities of domain name holders.
3. The ITA 2000 does not deal with issues concerning the protection of Intellectual Property Rights (IPR) in the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes. Thus, the law lacks "Proper Intellectual Property Protection for Electronic Information and Data" – the law misses out the issue of IPR, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. However, the corresponding provisions are available under the Indian Copyright Act (refer to Appendix T in CD).
4. As the cyberlaw is evolving, so are the new forms and manifestations of cybercrimes. The offenses defined in the ITA 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the ITA 2000 makes it appear as if the offenses detailed therein are the only cyberoffenses possible and existing. The ITA 2000 does not cover various kinds of cybercrimes and Internet-related crimes. These include:
 - Theft of Internet hours (see for more details in Chapter 1);
 - cybertheft;
 - cyberstalking (for more details refer to Section 2.4 of Chapter 2);
 - cyberharassment;
 - cyberdefamation (for more details refer to Section 1.5.3 of Chapter 1);
 - cyberfraud (for more details see Chapter 1);
 - misuse of credit card numbers;
 - chat room abuse;
 - cybersquatting (not addressed directly).
5. The ITA 2000 has not tackled vital issues pertaining to E-Commerce sphere like privacy and content regulation to name a few.
6. The Information Technology Act is not explicit about regulation of Electronic Payments, and avoids applicability of IT Act to Negotiable Instruments. The Information Technology Act stays silent over the regulation of electronic payments gateway and rather segregates the negotiable instruments from the applicability of the IT Act. This may have major effect on the growth of E-Commerce in India. This has led to tendencies of banking and financial sectors being irresolute in their stands.
7. IT Act does not touch upon antitrust issues.
8. The most serious concern about the Indian Cyberlaw relates to its implementation. The ITA 2000 does not lay down parameters for its implementation. Also, when Internet penetration in India is extremely low and government and police officials, in general, are not very computer savvy, the new Indian cyberlaw raises more questions than it answers. It seems that the Parliament would be required to amend the ITA 2000 to remove the gray areas mentioned above.

6.5 Challenges to Indian Law and Cybercrime Scenario in India

In the previous section, weak areas of the Indian IT Act were discussed. In that context note that the Indian Law does not provide any definition to the term *cybercrime*. In fact, the IPC does not use the term *cybercrime* at any point even after its amendment by the ITA 2000, supposedly, the Indian cyberlaw. On the contrary, it has a separate Chapter XI entitled *Offences* in which cybercrimes have been declared as penal offenses punishable with imprisonment and fine. The offenses covered under CHAPTER XI of the Indian ITA 2000 include:

1. Tampering with the computer source code or computer source documents;
2. un-authorized access to computer (“hacking” is one such type of act);
3. publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the prurient interest;
4. failure to decrypt information if the same is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign state, public order or for preventing incitement to the commission of any cognizable offense;
5. securing access or attempting to secure access to a protected system;
6. misrepresentation while obtaining, any license to act as a Certifying Authority (CA) or a digital signature certificate;
7. breach of confidentiality and privacy;
8. publication of digital signature certificates which are false in certain particulars;
9. publication of digital signature certificates for fraudulent purposes.

There are legal drawbacks with regard to cybercrimes addressed in India – there is a need to improve the legal scenario. These drawbacks prevent cybercrimes from being addressed in India. First, the difficulties/ drawbacks with most Indians not to report cybercrimes to the law enforcement agencies because they fear it might invite a lot of harassment. Second, their awareness on cybercrime is relatively on the lower side.

Another factor that contributes to the difficulty of cybercrime resolution is that the law enforcement agencies in the country are neither well equipped nor knowledgeable enough about cybercrime. There is a tremendous need for training the law enforcement agencies in India. Not all cities have cybercrime cells. Most investigating officers with the Police force may be well equipped to fight cybercrime.

We need dedicated, continuous and updated training of the law enforcement agencies. There is a lack of dedicated cybercrime courts in the country where expertise in cybercrime can be utilized. There is a need to strengthen the legal scenario in India. It is not adequate to merely enact a law. The law may even be theoretically effective; however, it is of no use if the law is not enforced with true rigor and spirit. Thus, yet another dimension of current challenges in India is that the current law enforcement machinery is not yet well equipped to deal with cyberlaw offenses and contraventions. There is also a crying need for cyber-savvy judges. Judiciary plays a vital role in shaping the enactment according to the order of the day. The cyber cell officials need a sound technical training along with suitable technological support. Preservation of law and order in the society depends heavily on a sound judicial system. A sound cyberlaw training to the judges and lawyers will go a long way in effective enforcement of cyberlaws.

There is a need for a distinct law on cybercrime and appropriate changes should be made in the IPC and the Information Technology Act. Uniform guidelines on cyberforensics tools and strategies should be circulated among investigating officers of cybercrime in the country. There is also a need to expedite

cybercrime trials. As a country, we need to learn constantly from the ever-growing developments in cybercrime all across the world. Fundamentally, what is required is training and orientation of the judiciary and the lawyers. We are still far away from being in the state of “Ideal Cyber Law in India.” To achieve that dream, it will require time, money and trained resources. There are good deal of efforts being done in this area and in the near future, the picture of our ability to fight cybercrimes is going to change considerably to rise up to the challenge.

People need to be encouraged to report the matter to the law enforcement agencies with full confidence and trust and without the fear of being harassed. There is perception issue too; the law enforcement agencies dealing with cybercrime need to come up with an extremely tech-savvy and friendly image. The Indian law enforcement agencies can follow the example set by the Federal Bureau of Investigation (FBI) in the US and go all out to strengthen the confidence of the people and companies who report cybercrimes to them. This should be possible because it is promised that complete secrecy would be maintained about all companies and people who report and assist in the investigation. We require apt laws and a proactive approach of the law enforcement agencies to effectively deal with the menace of cybercrime.

Whether the Indian law is practical and helpful in helping to solve cybercrime is a debatable topic. It is difficult to comment on this point. It is indeed helpful in addressing some cybercrimes, and in that sense the law is indeed practical. However, in the areas where the law does not cover some cybercrimes that have already emerged, the law is of no assistance or help whatsoever. The law enforcement agencies have been facing tremendous problems trying to cope with the challenges of emerging cybercrime within the ambit of the IPC, even if a liberal interpretation of it is taken. However, it is important to note that the Law alone does not help in punishing cybercrimes. It only prescribes punishments of various acts of cybercrimes. These acts are made punishable by imprisonment and fine. There are cases where the Indian cyberlaw has not prescribed punishments but has made these acts a ground for claiming compensation from the perpetrator of those acts. For example, if a computer virus is released and any damage caused, the cybercrime is punishable with imprisonment and fine. On the contrary, it can be made a ground for seeking damages up to ₹ 1 crore (₹ 1,00,00,000) against the perpetrator, provided his identity is known. As far as the issue of solving cybercrime goes, the onus lies with the law enforcement agencies and their will to do so. By and large, they are not well equipped enough to deal with cybercrimes and they do not possess the latest forensics tools. If our law enforcement agencies did have the requisite tools and the will, their success rate would indeed be better.

6.6 Consequences of Not Addressing the Weakness in Information Technology Act

In light of the discussion so far, we can see that there are many challenges in the Indian scenario for fight with cybercrime. Cyberlaws of the country are yet to reach the level of sufficiency and adequate security to serve as a strong platform to support India's E-Commerce industry for which they were meant. India has lagged behind in keeping pace with the world in this regard. The consequences of this are visible – India's outsourcing sector may get impacted. There are many news about overseas customer worrying about data breaches and data leakages in India. This can result in breaking India's IT business leadership in international outsourcing market.

Outsourcing is on the rise; if India wishes to maintain its strong position in the global outsourcing market, there should be quick and intelligent steps taken to address the current weaknesses in the Information Technology Act. If this is not addressed in the near future, then the dream of India ruling the world's outsourcing market may not come true.

6.7 Digital Signatures and the Indian IT Act

In this section, some potential problems regarding the terms *digital signatures* and *electronic signatures* are discussed. Public-key certificate and the role of public-key infrastructure (PKI) are also explained. Impact of oversights in ITA 2000 regarding digital signatures is also discussed. For the benefit of readers without technical background, the PKI and related terms are explained. For the discussion in this section, we will refer to Table 1.1 of Chapter 1 (Cybercrimes/Cases Registered and Persons Arrested under IT Act during 2004–2007); there is a mention of “publishing false digital signature certificate,” that is, item No. 7 in that table. CHAPTER XI (Offences) of the Indian IT Action mentions “penalty for publishing false digital signature certificate in certain particulars.” With those threads, in this section we will discuss particularly about digital signatures in context of the Indian IT Act. Before we do that, we need to understand a few technical concepts.

6.7.1 Public-Key Certificate

A public-key certificate is a digitally signed statement from one entity, saying that the public key (and some other information) of another entity has some specific value. A digital signature is a type of electronic signature that is used to guarantee the integrity of the data. When linked to the identity of the signer – using a security token such as X.509 Certificates – a digital signature can be used for non-repudiation, since it links the signer with the signed document. An X.509 Certificate contains information about the certificate subject and the certificate issuer (the CA that issued the certificate). A certificate is encoded in Abstract Syntax Notation One (ASN.1), a standard syntax for describing messages that can be sent or received on a network. The role of a certificate is to associate an identity with a public-key value. A certificate includes:

1. X.509 version information;
2. a serial number that uniquely identifies the certificate;
3. a common name that identifies the subject;
4. the public key associated with the common name;
5. the name of the user who created the certificate, known as the subject name;
6. information about the certificate issuer;
7. signature of the issuer;
8. information about the algorithm used to sign the certificate;
9. some optional X.509 version 3 extensions. For example, an extension exists that distinguishes between CA certificates and end-entity certificates.

Some of the most widely visible application of X.509 Certificates today is in Web browsers (such as Netscape Navigator and Microsoft Internet Explorer) that support the Secure Socket Layer (SSL) Protocol. SSL is a security protocol that provides privacy and authentication for your network traffic. These browsers can only use this protocol with web servers that support SSL. Other technologies that rely on X.509 Certificates include:

1. Code-signing schemes, such as signed Java Archives and Microsoft Authenticode;
2. Secure E-Mail standards, such as privacy-enhanced mail (PEM) and secure/multipurpose Internet mail extensions (S/MIME);
3. E-Commerce protocols, such as secure electronic transactions (SET).

Box 6.13 X.509 Digital Certificates

X.509 was initially issued on July 3, 1988 and was begun in association with the X.500 standard. It assumes a strict hierarchical system of Certifying Authorities (CAs) for issuing the certificates. This contrasts with web of trust models, like PGP, where anyone (not just special CAs) may sign and thus attest to the validity of others' key certificates. Version 3 of X.509 includes the flexibility to support other topologies like bridges and meshes (RFC 4158). It can be used in a peer-to-peer, OpenPGP-like web of trust, but was rarely used that way as of 2004. The X.500 system has never been fully implemented, and the IETF's public-key infrastructure (X.509), or PKIX, working group has adapted the standard to the more flexible organization of the Internet. In fact, the term X.509 Certificate usually refers to the IETF's PKIX Certificate and CRL Profile of the X.509 version 3 certificate standard, as specified in RFC 5280, commonly referred to as PKIX for public-key infrastructure (X.509). In the X.509 system, a CA issues a certificate binding a public key to a particular *Distinguished Name* in the X.500 tradition, or to an Alternative Name such as an E-Mail address or a DNS-entry.

In cryptography, X.509 is an ITU-T standard for a public-key infrastructure (PKI) for single sign-on (SSO) and privilege management infrastructure (PMI). X.509 specifies, among other things, standard formats for public-key certificates, certificate revocation lists (CRLs), attribute certificates and a certification path-validation algorithm.

Note: For Cryptography and Digital Signature Concepts, see Ref. #7, Books, Further Reading.

6.7.2 Representation of Digital Signatures in the ITA 2000

ITA 2000 had prescribed digital signatures based on Asymmetric cryptosystem and Hash system as the only acceptable form of authentication of electronic documents recognized as equivalent to "signatures" in paper form. When the ITA 2000 was drafted, there was a slip-up in the drafting of Section 35, subsection (3), which made it mandatory for an applicant of a digital signature certificate to enclose a *Certification Practice Statement* along with his application. One of the major deficiencies in the bill, which could hinder implementation, is the provisions regarding the role and function of the CAs as well as the process of issuing digital certificates.

Box 6.14 ITA 2000 Oversight

1. Licensing of Certifying Authorities (CAs)

Section 21 of the Act defines the licensing procedure for CAs. According to the provisions, the applicant for such a license should fulfill the requirements of "qualifications," "expertise," "manpower," "financial resources" and "other infrastructural facilities," which are necessary to issue digital certificates as may be prescribed by the Central Government. Furthermore, "The license will be valid for such period as may be prescribed by the Central Government and would not be transferable or heritable."

Considering the responsibilities that a CA has to discharge, the business of the CAs will involve a heavy investment in terms of infrastructure, manpower and marketing. The licensing period, therefore, has to be long enough to make the business viable. If this is as short as say 1 year, no CA will be able to break even before his first license expires. He will then come up for assessment for the renewal application and judged based on his performance, which may not be reflective of his potential.

In the absence of transferability, he may even be restrained from upgrading his skills through a joint venture partner. If the CA finds it uneconomical to run the business, he will even be prevented from handing over the business to another more efficient entity. In such an event, it would be the Netizens holding certificates issued by such a vacating CA who may suffer.

It is, therefore, necessary that the initial licensing period should be atleast 5 years and no restrictions be placed on the transferability of the ownership of the company that is granted the license. The Controller may, however, retain the right to review the license if he feels that the changes may compromise the interest of the customers of the erstwhile company.

Box 6.14 ITA 2000 Oversight . . . (Continued)

2. Licensing of foreign CAs

In view of the enormous preparations required to set up the CAs business, Indian CAs will take some time to come up with their services. Until such time, the market has to be supported by the foreign CAs. Otherwise, even after the Act is finally in place, it cannot be implemented in the absence of the digital signature infrastructure.

Sadly, the bill has made the task of getting license by foreign CAs unnecessarily complicated and needs an immediate review.

As per the bill, certificates will not be valid unless the issuing CA is approved by the Controller. For a foreign CA to get the approval, he has to open a physical office in India where he has to display (!) the license (Section 32). Before approving the foreign CA, the Controller has to obtain the permission of the Central Government and the fact should be notified in the Gazette.

Whoever drafted the above provision seems to have overlooked the ground realities. First, there are already many users in India who have obtained individual or secured server digital certificates from foreign CAs such as Verisign. Now, if for argument sake, Verisign does not get the license as a CA from the Controller in India; the existing certificates issued by them will not be valid under the Indian law.

Similarly, if an Indian who has obtained a certificate from a licensed CA has to enter into a contract with an Australian counterpart who has a certificate from an Australian CA, the contract may not be considered valid under the Indian cyberlaw unless the Australian CA also obtains license in India.

Will all the certification authorities in every other country agree to open offices in India, apply for license, wait for the government to approve and notify in the Gazette and display the certificates in their Indian offices? The answer is a definite "impossible."

It is, therefore, appropriate if (as is prevailing in some other countries) the validity of certificates from any CA already approved in other countries is automatically extended to India.

3. Do Individuals need to submit Certification Practice Statement?

If the provisions discussed above display only the ignorance of the lawmakers, the reading of Clause 35 leaves one wondering how such blatant errors have gone un-noticed to become law. This section deals with issue of digital certificates by the CAs. Surprisingly, Clause 35.3 says, "Every Such application shall be accompanied by a certification practice statement . . .".

Obviously, the Clauses 35.2 and 35.3 have been borrowed from the clause meant for the processing of an application of a CA requesting a license to issue digital certificates. The wording of Clause 35.4 further indicates that this faux pas is not just a slip but a deliberate insertion in the belief that it is necessary.

These clauses have to be deleted and modified appropriately.

6.7.3 Impact of Oversights in ITA 2000 Regarding Digital Signatures

The oversights, explained in the previous section, result in serious concerns – it is troublesome to imagine what will happen when the rules under the act are drafted. To keep the situation under control, the Ministry of Information and Technology had to urgently establish a task force to assist them in the drafting of the rules. The task force consisted of experts in the field. It is said that now this blunder has been accompanied by more avoidable confusions. Let us understand this. The Information Technology Amendment Bill 2006 was drafted on the basis of the recommendations of an "Expert Committee." The Committee took into consideration a recommendation from technical community that (a) the PKI-based system made the law dependent on a single authentication technology and (b) there was a need to make the law *Technology Neutral* (see Box 6.15 and Box 6.16).

Box 6.15 Digital Signature and Public-Key Infrastructure Technology

Modern day business transactions are computer-based, therefore, IT security services based on cryptography become essential. Public-key cryptography can play an important role in providing needed security services including confidentiality, authentication, digital signatures and integrity. Public-key cryptography uses two electronic keys: a *public key* and a *private key*. These keys are mathematically related but the private key cannot be determined from the public key. The public key can be known by anyone while the private key is kept secret by its owner.

As long as there is strong binding between the owner and the owner's public key, the identity of the originator of a message can be traced to the owner of the private key. A PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public-key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable CA.

The widespread use of PKI technology to support digital signatures can help increase confidence of electronic transactions. For example, the use of a digital signature allows a seller to prove that goods or services were requested by a buyer and therefore demand payment. The use of a PKI allows parties without prior knowledge of each other to engage in verifiable transactions.

For example, a buyer interested in purchasing certain goods from company A electronically would need to obtain a public-key certificate from a CA. In one possible scenario, the buyer would generate a public-private key pair, provide a Registration Authority (RA) with a valid photo ID and ask for a certificate. The RA would verify the buyer's identity based on the photo ID and vouch for the identity of the buyer to a CA, who would then issue the certificate. The newly certified buyer can now sign electronic purchase orders for the goods ordered. The vendor of those goods receiving the purchase order can obtain the buyer's certificate and the Certificate Revocation List (CRL) for the CA that issued the buyer's certificate, check that the certificate has not been revoked, and verify the buyer's signature. By verifying the validity of the certificate, the vendor ensures receipt of a valid public key for the buyer; by verifying the signature on the purchase order, the vendor ensures the order was not altered after the buyer issued it.

Once the validity of the certificate and the signature are established, the vendor can ship the requested widgets to company A with the knowledge that their buyer ordered the widgets. This transaction can occur without any prior business relationship between the buyer and the seller. Potentially, a user's private-public key pair can be used for multiple applications. For example, the same key used to sign the purchase order could be used by the buyer to authenticate an electronic payment to the vendor through the buyer's bank.

Most of the processing in the above example can occur automatically depending on the application. After obtaining a certificate, perhaps a click on an icon is all it takes for a user to sign a message. Similarly, the verification process on the receiver's end would occur as a message is received without requiring much intervention from the person receiving the message.

Box 6.16 PKI – Basic Components

The PKI technology has the six basic components:

1. **Public-key certificate:** It is an electronic record that binds a public key to the identity of the owner of a public-private key pair and is signed by a trusted entity.
2. **Certificate revocation list (CRL):** It is a list of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example, a certificate can be revoked if the owner's private key has been lost or if the owner's name changes.
3. **Certification Authority (CA):** A trusted entity that issues and revokes public-key certificates and CRLs.
4. **Registration Authority (RA):** An entity that is trusted by the CA to register or vouch for the identity of users to a CA.

Certificate repository: An electronic site that holds certificates and CRLs. CAs post certificates and CRLs to repositories.

Certificate user: An entity that uses certificates to know, with certainty, the public key of another entity.

To honor this recommendation, the Committee tried to define an umbrella system of “electronic signatures” of which “digital signature” was one of the kinds. In consideration of this, in the Information Technology Amendment Bill 2006, Clause 2, a list of amendments were proposed to replace the word *digital* with the word *electronic* at several places in the principal act where a reference to “digital signature” had been made. However, somewhere along the line, some changes were made which are now appearing as anomalies in the legislation passed.

6.7.4 Implications for Certifying Authorities

The bill needed further amendments based on the Standing Committee report. To address that, instead of drafting a new amendment bill, a bill called “Information Technology Amendment Bill 2008” was drafted and it was introduced in the parliament on 15 December 2008. This bill passed certain amendments to the then pending Information Technology Amendment Bill 2006 (introduced on 15 December 2006) including the name clause of the resulting Act as in the bill introduced on 15 December 2006 which was changed from “Information Technology Amendment Act 2006” to “Information Technology Amendment Act 2008.” In the process of drafting an amendment bill (which was meant for amending a pending bill that was to amend a prevalent act), some serious slip-ups have crept into the Act which is now a law.

Instead of the earlier proposal to call “digital signature” as one type of an umbrella kind “electronic signature,” the current draft introduced a new Section 3A to define *electronic signatures* and retained the earlier Section 3 of *digital signatures*. This has made “electronic signature” a concurrent alternative proposed by law to “digital signature” and both could be used for authentication of electronic documents. As a result, the CAs’ regulations also need to be accommodated for both digital signature as well as electronic signature. Either the current CAs need to be licensed for “electronic signatures” also or there may be new CAs who only apply for being CAs for “electronic signatures” and not opt for having any “digital signature products.”

Public should also be able to “affix digital signature” and “affix electronic signature” as the case may be. They can acquire two different certificates, one for digital signature and the other for electronic signature, which may involve different CAs. The law, therefore, needs to accommodate all these provisions. It appears that the drafting of the bill has resulted in some confusion whereby in some places the digital signature and electronic signature are mentioned together and in some places they are mentioned differently. The net result is inconsistent treatment giving rise to anomalies that could have been avoided.

Section 3A: Electronic Signature

- (1) Notwithstanding anything contained in Section 3, but subject to the provisions of subsection (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication that
 - (a) is considered reliable and
 - (b) may be specified in The Second Schedule.
- (2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if
 - (a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;
 - (b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
 - (c) any alteration to the electronic signature made after affixing such signature is detectable;
 - (d) any alteration to the information made after its authentication by electronic signature is detectable and
 - (e) it fulfills such other conditions which may be prescribed.

- (3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.
- (4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule.
Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.
- (5) Every notification issued under subsection (4) shall be laid before each House of Parliament.

6.7.5 The Current Scenario Regarding Digital Signatures under the Indian IT Act

At present, there is no system of electronic signature defined in the Second Schedule and therefore there is no change in the authentication mechanism under the Act. As a result, the present system of digital signatures will continue for the time being and will be the only method of authentication of an electronic document. When the government needs to introduce a new system, it will have to notify through the Official Gazette the relevant procedure that can be considered as reliable. This would also require the notification to be placed before the Parliament.

Obviously, the system should meet the minimum criteria of effectively establishing the authentication of a document to the person who authenticates it and also should ensure that if the document has been changed since it was signed, such alteration becomes noticeable. If we go by the reliability of the Hash algorithms and the Asymmetric cryptosystems used for the current digital signature system that are reviewed worldwide by mathematicians on a regular basis, any alternative system should also meet similar stringent standards. In other words, if any technical solutions need to be considered as a concurrent alternative to the present PKI-based system, then the system has to be not only put to extensive tests within India but also in global circles. Additionally, the system has to be licensed in a manner similar to the manner of licensing CAs at present. We may, therefore, either see the current CAs who may introduce new systems or exclusive “Electronic Signature Certifying Authorities” who may seek license from the government and function along with the current “Digital Signature Certifying Authorities.”

However, in the near future, the digital signature system will continue to be the sole system of authentication that would be recognized by Indian law. Thus, the need for “digital signature system” to continue for the time being, results in some serious legal lacuna. In Section 2(d) of the new Act, “affixing of an electronic signature” is defined as

“Affixing Electronic Signature” with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature

There is, however, no corresponding definition for “affixing of a digital signature.” Fortunately the definition of “digital signature” and “digital signature certificate” remains under Section 2(p) and 2(q) while the definition of “electronic signature” and “electronic signature certificate” has been added under Sections 2(ta) and 2(tb). In Sections 2(ta) and 2(tb), the definition of “electronic signature” and “electronic signature certificate” is given as “includes digital signature” or “digital signature certificate,” respectively. This does not mean that the two terms are same; however, the system used in digital signature is considered “reliable” as per Section 3A of the new Act. Owing to the inclusion of digital signature in Sections 2(ta) and 2(tb), the

regulations regarding CAs mentioning *electronic signatures* will be applicable for digital signatures. However, regulations meant for *digital signatures* may not all be applicable to electronic signatures and their issuers.

Sections 37, 38 and 39, meant for suspension and revocation of digital signatures, do not automatically apply for electronic signatures. Although Section 40A specifically speaks of an intended amendment when electronic signature becomes a reality, similar new Sections 37A, 38A and 39A are required in such an event. Additionally, many more sections where only “digital signature” has been mentioned need to be supported by additional sections for electronic signatures. In particular, Section 21, which talks about licensing of CAs, itself needs to be supported with a corresponding section for electronic signatures.

Therefore, as and when procedures for electronic signatures were introduced, several sections needed to undergo changes. This has been another major amendment to the Act. Some of these difficulties could have been avoided by replacing the word “digital signature” by the words “digital signature and electronic signature where relevant” in Clause 2 of the IT Amendment Bill 2006. Now it appears that perhaps clubbing of the terms “digital signature” and “electronic signature” under Section 2 could have been avoided.

The law could have just made an enablement of an alternative to digital signatures and left other things to be added as and when any new system of electronic signature comes for consideration. At this point of time, we are not sure as to (a) what kind of systems can substitute or work along with digital signatures and (b) what kind of changes would be required in the law to accommodate them. The legal confusions created by this may also impact interpretations in “Indian Evidence Act” and there may be interesting battles of interpretations that will confuse and confound legal and judicial officers in courts. If the final draft of the bill had been debated in public space for some time rather than being hurriedly pushed through the Parliament, perhaps some of these confusions could have been avoided.

6.7.6 Cryptographic Perspective on the Indian IT Act

To appreciate the discussion in this section, readers need to be familiar with cryptography and encryption; these aspects are explained in Ref. #7, Books, Further Reading. A few shocking dimensions of digital signatures are explained here.

In plain language, non-repudiation means the assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Technically speaking, the term *non-repudiation* has a specific meaning in E-Commerce; it means the intent to accept responsibility of submitting or receiving an electronic message and be bound by its substance. Non-repudiation in E-Commerce systems and electronic messaging systems is important because it protects a sender against the false assertion of the receiver that the message has not been received, and also protects a receiver against the false assertion of the sender that the message has been sent. Theoretically, public-key-based digital signatures are “non-repudiable” and this is one of their most frequently cited benefits. However, when you send an electronic message over the Internet, your digital signature does not prove that you signed the message – it only means that your private key got attached to that message. When talking about “non-repudiation,” an often ignored aspect is that there is something between you and your key and your computer system. If your computer system were infected, the Malicious Code could use your key to sign documents without your knowledge or permission! Even if you wanted to give explicit approval for each signature (e.g., via a fingerprint scanner), the Malicious Code could wait for you to approve a signature and would then sign its own message instead of yours. If the private key is not in tamper-resistant hardware, the Malicious Code can just steal the key as soon as it is used.

Such details may get legitimately ignored in cryptographic designs. It would be wrong to assume that real computer systems implement the theoretical ideal. Your computer may contain viruses. Without due care, your computer may also be accessible to passers-by who could plant Malicious Code or manually sign things with your keys. In such a scenario, if we needed to deny some signature, we would owe the burden of proving the negative, that is, we did not make the signature in question against the presumption that we did. The main risk in believing this popular falsehood stems from the cryptographic concept of “non-repudiation”; so let us revisit the meaning of this term. There are two following definitions for the term *non-repudiation*:

1. **Definition 1 (General):** The intent to accept one's obligation under a contract and be bound for its performance.
2. **Definition 2 (E-Commerce):** The intent to accept responsibility of submitting or receiving an electronic message and to be bound by its substance. Non-repudiation protects a sender against the false assertion of the receiver that the message has not been received and a receiver against the false assertion of the sender that the message has been sent. An essential element of secure E-Commerce, non-repudiation is generally established by the protocol [such a PKI or EDIFACT (see Box 6.17) used in data transfer], and includes legal and security criteria of authentication and report integrity.

Box 6.17 EDIFACT Basics

EDIFACT is an acronym for *EDI for Administration, Commerce and Transport* (EDIFACT). It coordinates international standardization by working through the UN/ECE (United Nations/Economic Commission for Europe). The EDIFACT standard provides:

1. An international EDI standard that works as a set of syntax rules to structure data;
2. an Interactive Exchange Protocol (I-EDI);
3. a set of syntax rules;
4. data elements, segments and codes;
5. standard messages which allow multi-country and multi-industry exchange.

EDIFACT has a hierarchical structure where the top level is referred to as an interchange, and lower levels contain multiple messages which consist of segments, which in turn consist of composites. EDIFACT has been adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735. An example of an EDIFACT message used to answer to a product availability request is mentioned below:

```

UNB+IATB;1+6XPPC+LHPPC+940101:0950+1'
UNH+1+PAORES:93:1:IA'
MSG+1:45'
IFT+3+XYZCOMPANY AVAILABILITY'
ERC+A7V:1:AMD'
IFT+3+NO MORE FLIGHTS'
ODI
TVL+240493:1000::1220+FRA+JFK+DL+400+C'
PDI++C:3+Y::3+F::1'
APD+74C:0::6++++++6X'
TVL+240493:1740::2030+JFK+MIA+DL+081+C'
PDI+C:4'
APD+EM2:0:1630::6++++++DA'
UNT+13+1'
UNZ+1+1'

```

Recall that we mentioned two definitions of the term *non-repudiation*. Now let us further understand the traditional legal meaning of “non-repudiation.” There is a definitional *distinction between the legal use of the term “non-repudiation” and its crypto-technical use*. First, let us consider the legal use of the term. In the legal sense, an alleged signatory to a document is always able to repudiate a signature that has been attributed to him or her. The basis for a repudiation of a traditional signature may include:

1. The signature is a forgery.
2. The signature is not a forgery, but was obtained via
 - Unconscionable conduct by a party to a transaction;
 - fraud instigated by a third party;
 - undue influence exerted by a third party.

The common law trust mechanism established to overcome a false claim of non-repudiation is *witnessing*. Witnessing may simply occur at the point of the signature being affixed, that is, with the presence of an independent adult to witness the signing of a document reduces the ability of the signatory to successfully deny the signature as a forgery at a later date. It is always open for the signatory to deny the signature on other grounds such as those already enumerated.

An issue arises whether a digital signature should be treated differently compared with a traditional signature. In the E-Commerce environment, it is presumed that the law should not alter this position with regard to the legal rights of parties to repudiate a digital signature. Governments worldwide have consistently supported this position. The E-Commerce environment should not have different rules from those developed over many centuries in the paper-based environment. These rules have been developed as well as judicially tested to avoid disadvantage to any party in a transaction. Now let us consider the crypto-technical meaning of “non-repudiation.” In general terms, it means

1. In authentication, a service that provides proof of the integrity and origin of data, both in an unforgeable relationship, which can be verified by any third party at any time; or
2. in authentication, an authentication that with high assurance can be asserted to be genuine and that cannot subsequently be refuted.

Coming back to the topic of sending an electronic message over the Internet with “digital signature,” PKI has been overtouted as the solution to many network security problems. It is known that there are problems that are beyond PKI’s ability to solve; PKI solution vendors do not like this to be mentioned. The worst of all is if a country’s laws are framed in such a way that they make you liable (legally) if your private key is used to sign a document. In Section 42 of the Indian IT Act titled *Control of Private Key*, there is an explanation stating this: *For clarifying doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised*.

In spite of the “Controller of Certifying Authority” (CCA) and the CA certifying the digital signature, the total risks involved and the financial injury suffered by the citizen in accepting the digital signature is entirely with the person accepting the digital signature and NOT with the CA or CCA even if it was proved that it was due to the mistake of the CA or CCA.

The Indian ITA 2000 puts the liability on the person who accepts the digital signature (i.e., do it at your risk!). The only way to escape the misplaced legal liability is:

1. Never get your key certified by a CA;
2. never get your public key published for the benefit of the public;
3. never accept digital signature for things that involve legal liability; this does not prevent using digital signature between two trusted friends or partners.

To understand the risks involved in PKI, refer to Ref. #14, Additional Useful Web References, Further Reading.

6.8 Amendments to the Indian IT Act

In Section 6.7.5 we explained about the issue regarding digital signature in the Indian IT Act. There are other aspects as well. According to some experts, Indian law may satisfy European Union's data protection concerns. For example, to win the business in global market, it is essential to create appropriate confidence among investors and foreign companies to assure them that the data sent to India for backoffice operations will indeed be safe, and there are appropriate statutory mechanisms in place should a breach of data take place. Due to this, it is becoming extremely important for India to have in place a distinctive legal regime promoting data protection. In this context, Example 11 in Section 11.2.11 in Chapter 11 brings the following key point to the table:



Indian BPO organizations are classified as *intermediaries* and as such they do have liabilities in case of breached data.

A welcome change is heralded by the amendments to the Indian IT Act. So far, Information Security Experts have been speaking about *cyberlaw compliance* as a part of *Techno Legal Information Security* and advising Companies to formulate an appropriate action plan to comply with cyberlaws as a part of the information security practice. Now this association of cyberlaw with the information security domain has gained additional importance due to some amendments that have been made to ITA 2000.

As a quick note, in the amended Indian IT Act, that is, the ITA 2008 (year 2008 amendments to the Indian IT Act), there is addition of several new offenses that are apt with the new paradigm in today's net-centric digital economy. Section 66 has now been expanded to include Sections 66A (*Offensive Messages*), 66B (*Receiving Stolen Computer*), 66C (*Identity Theft*), 66D (*Impersonation*), 66E (*Violation of Privacy*) and 66F (*Cyber Terrorism*). Section 67 has been expanded to include Sections 67A (*Sexually Explicit Content*) and 67B (*Child Pornography*). However, with these additional sections, police may have some concerns; for example, one such concern could be that under Section 78, now inspectors can undertake investigations of cybercrimes under the Act. This means that it would not only be the DSPs who need to be trained in ITA 2000 but all the inspectors in the state. The implication is that now the training requirements would again grow manifolds. In the paragraphs that follow, we provide an overall outlook on the changes (amendments) made to the Indian IT Act. We have provided a running commentary on Sections 43, 67C, 66B, 69B, 70B(4), 70B(6), 70B(7), 72A, 78, 80 and 85 of the amended IT Act.

First, let us revisit the term *cybersecurity* – in authors' opinion, the amended IT Act makes a sincere effort to consider complete information security infrastructure that exists in the industry. The new legal definition that given to the term *cybersecurity* under the newly inserted Section 2(nb) (Inserted Vide ITAA 2008) – "*Cyber Security*" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

A Glimpse into Indian IT Act Amendment

Section 2(nb) (Inserted Vide ITAA 2008)

"Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction."

To support the development of the cybersecurity infrastructure, the amendments also focus on

1. Defining penalties for violation;
2. defining appropriate level of compensation;
3. setting up an authority for implementation.



The term *cybersecurity* incorporates both the physical security of devices as well as the information stored therein. It covers “protection from unauthorized access, use, disclosure, disruption, modification and destruction.”

To support the development of the cybersecurity infrastructure, the amendments also focus on

1. Defining penalties for violation;
2. defining appropriate level of compensation;
3. setting up an authority for implementation.

As far as “penalties for violation” are concerned, a new offense has been defined, to recognize the need to expressly penalize the “theft” of computer or other communication devices.



Under the newly added Section 66B, the receiver of a stolen computer resource may be liable for punishment.

6.8.1 Overview of Changes Made to the Indian IT Act

Section 66B of the Amended IT Act of India

Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008) is presented below.

A Glimpse into Indian IT Act Amendment

Sec 66B: It states punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008):

“Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.”

Thus, under Section 66B, receiving a stolen computer or a mobile or even a CD or an E-Mail containing stolen information is liable to punishment with 3 years of imprisonment. The offense would be cognizable

and compoundable. A person becomes liable when he/she receives the information “dishonestly” and is aware that it is “stolen.” This section empowers the police force as they can now book all mobile theft or laptop theft cases under this section. So far, attempts were made to convince the police that any theft of computer device would be “diminishing the value of information residing therein” and therefore should be booked under Section 66. Now it may be easy to convince the police.

Sections 78 and 80 of the Amended IT Act of India

Along with the changes made to Sections 78 and 80 of the ITA 2000, bringing down the authority of investigation from the level of DSPs to the level of inspectors, the number of complaints that need to be registered under “cybercrimes” are now expected to grow considerably in numbers. Therefore, the police may now need to work overtime and will also need to get trained in handling of cybercrimes.

A Glimpse into Indian IT Act Amendment

With the change made to Sections 78 and 80 of the ITA 2000, the authority of investigation is brought down from the previous level of DSPs to the level of inspectors. Now the number of complaints registered under “cybercrimes” are expected to increase manifolds and the police need to work overtime as well as get trained in the handling of cybercrimes.

Section 43 of the Amended IT Act of India

In addition to the provision under Section 66B mentioned above, this section, when read with other changes, increases the possibility of compensation from a maximum of ₹ 1 crore (₹ 10,000,000) to even beyond ₹ 5 crore (₹ 5,00,00,000). Although the fast track “adjudication” is restricted to cases where the compensation is up to ₹ 5 crore (₹ 5,00,00,000), there is no upper limit on the compensation to be claimed.

The newly added Section 43(j) tries to expand the cases where compensation can be claimed to cases when a person without the permission of the owner of a computer, computer resource “steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.”

A Glimpse into Indian IT Act Amendment

The newly added Section 43(j) tries to expand the cases where compensation can be claimed to cases of a person without the permission of the owner of a computer, computer resource “steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.”

1. **Meaning of source code:** “Computer source code” means “the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.”
2. **Advantage of this definition:** It makes it easy for police to understand how to treat a complaint from a software company about stolen data. The penalty for stolen data does not end with the perpetrator of the offense as far as the victim is concerned. The provisions on *data protection* extend the liability for lack of cybersecurity to the companies too.

A Glimpse into Indian IT Act Amendment – Compensation for Failure to Protect Data

Under the newly introduced Section 43A, “Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.”

Under the newly introduced Section 43A

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource, which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Note that there is no upper limit to the liability under this section. In understanding the responsibilities under this section, the term *reasonable security practices* becomes vital. As per the explanation to the section, *reasonable security practices and procedures* means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

A Glimpse into Indian IT Act Amendment

As per the explanation to the section, “*reasonable security practices and procedures*” means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Section 72A of the Amended IT Act of India

Under this section, a provision has been made for criminal prosecution in the event of breach of information security. It is stated as

“Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term, which may extend to three years or with a fine, which may extend to five lakh rupees or with both.”

Note again that this offense is cognizable.

A Glimpse into Indian IT Act Amendment

Under Section 72A, there is a provision for Criminal prosecution for breach of information security. This section states, “*Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.*”

Section 85 of the Amended IT Act of India

The principle of “vicarious liability” is based on the concept of causing a damage or injury due to negligence. The term *vicarious liability* is used to indicate that the law holds one person responsible for the misconduct of another, although the first person is free from any personal blameworthiness or fault. The legal principle of vicarious liability applies to hold one person liable for the actions of another when engaged in some form of joint or collective activity. Under Section 85, the organization as well as its directors or officers in-charge of business “shall be” held guilty of the offense committed “by the organization.” Thus, the “vicarious liability” on the companies for “data protection” has been hardened. See the bar below.

A Glimpse into Indian IT Act Amendment

Further under Section 85, the company as well as its Directors or officers in-charge of business “shall be” held guilty of the offense committed “by the company.”

Thus, the “vicarious liability” on the companies for “data protection” has been hardened.

Section 67C of the Amended IT Act of India

Under Section 67C, there is a further responsibility trusted with “intermediaries.” Intermediaries now include body “corporate” to retain information for a certain time as specified by the Central Government. The section reads:

Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. Any intermediary who intentionally or knowingly contravenes the provisions of subsection (1) shall be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine.

With regard to this, Example 11 in Section 11.2.11 in Chapter 11 should be read. A key point mentioned in that example is that Indian BPO organizations are classified as *intermediaries* and as such they do have liabilities in case of breached data.

A Glimpse of Indian IT Act Amendment

Under Section 67C, a further responsibility has been cast on “Intermediaries” (which now includes body corporates to retain information for a certain time to be specified by the Central Government. The section reads

- Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
- Any intermediary who intentionally or knowingly contravenes the provisions of subsection (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

This is an important provision to make ISPs, managed service providers (MSPs), responsible along with others who today seem to evade taking the responsibility of preserving information that would serve as evidence in case of cyberoffenses. The duration for which information has to be preserved, needs to be prescribed in the rules and notifications.

Section 69B of the Amended IT Act of India

To address the need for monitoring “cybersecurity,” it is stated that

“The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.”

It is important to note that the intermediary or any person in-charge of the computer resource shall when called upon by the agency, which is vested with power under subsection (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information. The procedure and safeguards for monitoring and collecting traffic data or information shall be such as may be prescribed. Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine.

A Glimpse into Indian IT Act Amendment

As a part of the need to monitor cybersecurity, under Section 69B,

- The Central Government may, to enhance cybersecurity and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorize any agency of the government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
- The intermediary or any person in-charge of the computer resource shall when called upon by the agency which has been authorized under subsection (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
- The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
- Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section, the term *computer contaminant* has the same meaning as was assigned to it in Section 43. *Traffic data* constitutes any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted. “Traffic data” includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information. Implementation mechanism: Apart from throwing open registration and investigation of cybercrimes to inspector level, at the national level, a new *nodal agency* comes into being for implementation of cybersecurity.

Section 70B(4) of the Amended IT Act of India

Under this section, it is stated that

The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security: collection, analysis and dissemination of information on cyber incidents forecast and alerts of cyber security incidents emergency measures for handling cyber security incidents coordination of cyber incidents response activities issue guidelines, advisories,

vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents such other functions relating to cyber security as may be prescribed.

A Glimpse into Indian IT Act Amendment

Under Section 70B(4), The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cybersecurity:

- Collection, analysis and dissemination of information on cyber incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- coordination of cyber incidents response activities;
- issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- such other functions relating to cybersecurity as may be prescribed.

Section 70B(6) of the Amended IT Act of India

The statement of the section is presented below. Note the terms “service providers,” “intermediaries,” “data centers” and “body corporate.”

A Glimpse into Indian IT Act Amendment

Under Section 70B(6), “*For carrying out the provisions of subsection (4), the agency referred to in subsection (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.*”

Section 70B(7) of the Amended IT Act of India

Under this section, it is stated that “*Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under subsection (6), shall be punishable with imprisonment for a term, which may extend to one year or with fine, which may extend to one lakh rupees or with both.*” The same is presented below.

A Glimpse into Indian IT Act Amendment

Under Section 70B(7), “*Any person who fails to provide the information called for or comply with the service provider, intermediaries, data centers, body corporate or direction under subsection (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.*”

Finally, to conclude the discussion of this section, we note that the cumulative effect of the above provisions of ITA 2008 is to create a new cybersecurity implementation infrastructure in India and it is considered a highly positive development in the industry. The next steps to be watched are of course how the provisions would be actually implemented through appropriate rules and regulations.

6.8.2 Cybercafe-Related Matters Addressed in the Amendment to the Indian IT Act

The background for cybercafe matters addressed in the Indian IT Act Amendment is interesting. On 29 May 2001 two persons (Jayesh Thakkar and Sunil Thacker) sent a letter to the Chief Justice of the Bombay High Court complaining about the proliferation of pornographic sites on the Internet. The letter was numbered as Writ Petition 2611 of 2001.

During the subsequent hearings, the Internet Users Association of India (IUAI) was permitted to intervene in the matter. The Government of Maharashtra and the Union Territory of India had also appeared in the court. On 28 September 2001, the Division Bench of the High Court presided over by the learned Chief Justice passed an order appointing a Committee to suggest and recommend ways, measures and means to protect/shield minors from access to pornographic and obscene material on the Internet.

Cybercafes continued to attract attention later too. There were several mails sent from a cybercafe threatening terrorist attacks on some of Bangalore's IT companies. In the past also, there have been many instances where E-Mails sent from cybercafes have been used either for real or false terrorist communication. Several cybercrimes including stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes. It was also noticed that cybercafes were regularly used to send obscene mails to harass people. The perceived advantage (from criminals' point of view) of using a cybercafe is that E-Mails are hard to track. We know how terrorists used the wireless technology in the November 2008 attacks in Mumbai (known as "11/26 attacks in Mumbai") and it is also known that the recent blasts in Ahmedabad are being traced to a cybercafe in Navi Mumbai (New Bombay). It is for this reason that cybercafe owners are supposed to ask for a or rather insist on proper identification and a contact telephone number as well. However, when we did an informal survey of cybercafes in one city, we found that hardly any such precautions were taken and we also found many other less than desirable practices prevalent in the cybercafes. One can understand why cybercafes have been considered as one of the key intermediaries which need to be regulated. To regulate cybercafes, several states had passed regulations – some under ITA 2000 and some under the State Police Act.

Moreover, the problem was that the Indian ITA 2000 had not defined cybercafes; so they could only be interpreted as "network service providers" under the erstwhile Section 79. This imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network. The concept of *due diligence* was interpreted from the various provisions in cybercafe regulations where available or under the normal responsibilities expected from network service providers. Now, the Information Technology Amendment Act 2008 has made many significant changes in the prevailing laws of cyberspace applicable in India, one of which is regarding cybercafes. The ITA 2008 has now provided a specific definition for the term *cybercafe* and also included cybercafes under the term *Intermediaries*. Several aspects of the Act therefore become applicable to cybercafes and there is a need to take a fresh look at what cybercafes are expected to do for cyberlaw compliance. This is explained in Table 6.8.

It is interesting to note that the Karnataka Regulation was notified under Section 90 of ITA 2000 whereas the Tamil Nadu Act was notified under the State Police Act. Now that ITA 2000 has been amended, the provisions under Karnataka Cybercafe Regulation may have to be considered while there may be a question mark on the validity of Tamil Nadu Regulations. Mumbai, Maharashtra and Gujarat who also have some state level regulations may also be in a state similar to that of Tamil Nadu.

Sections 69, 69A and 69B specifically vest the powers in an agency to be designated. They have deliberately avoided the use of the term *police*. The legislative intent is, therefore, indicative that police need not be the agency to exercise the powers under these sections.

Table 6.8 | ITA 2008 and cybercafes

<i>ITA 2008 Section</i>	<i>What it States</i>	<i>Comment</i>
Section 2(na)	“Cybercafe” means any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.	This definition is an improvement of what was earlier proposed by the Expert Committee and the first draft of ITAA 2006 that had several anomalies. However, this definition may conflict with the definitions given under the current regulations passed by various States. See Note 1 at the end of this table.
Section 2(w)	The definition of “Intermediaries” includes “Cybercafes.” The regulations for Intermediaries therefore apply to Cybercafes after ITA 2008 becomes effective.	
Section 67C	<ul style="list-style-type: none"> • Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. • Any intermediary who intentionally or knowingly contravenes the provisions of subsection (1) shall be punished with an imprisonment for a term that may extend to 3 years and shall also be liable to fine. 	Thus, the responsibility of Cybercafes has now been clearly defined with a three year imprisonment which is also cognizable, bailable and compoundable. See Note 2 at the end of this table.
Section 69 (modified version)	<ul style="list-style-type: none"> • Where the Central Government or a <i>State Government</i> or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the <i>commission of any cognizable offence</i> relating to above or for investigation of any offence, it may, subject to the provisions of subsection. • For reasons to be recorded in writing, by order, direct any agency of the appropriate Government to <i>intercept, monitor or decrypt</i> or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource. • The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed. 	See Note 3 at the end of this table

(Continued)

Table 6.8 | (Continued)

<i>ITA 2008 Section</i>	<i>What it States</i>	<i>Comment</i>
69A	<ul style="list-style-type: none"> • The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency that has been directed under subsection (1), extend all facilities and technical assistance to <ul style="list-style-type: none"> • Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or • intercept or monitor or decrypt the information, as the case may be; or • provide information stored in computer resource. • The subscriber or intermediary or any person who fails to assist the agency shall be punished with an imprisonment for a term which may extend to 7 years and shall also be <i>liable to fine</i>. • Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient to do so in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of subsections. • For reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource. • The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed. • The intermediary who fails to comply with the direction issued under subsection (1) shall be punished with an imprisonment for a term that may extend to 7 years and also be liable to fine. 	<p>The important points to be noted in this section as well as the two other Sections 69A and 69B (quoted below) are</p> <ul style="list-style-type: none"> • These powers are available to both the Central and State Governments who can specially authorize an officer for the purpose. • It can be invoked even for preventing incitement to the commission of any cognizable offence. It is debatable whether the term Cognizable Offence has to be restricted to ITA 2008 only or can be extended to Indian Penal Code or other laws as well. • Government shall prescribe necessary safeguards to be followed by Intermediaries. • The powers include demanding of information stored in a computer. • Non-compliance may result in stiff penalty of imprisonment up to 7 years.
69B	<p>The Government now will have powers to collect "Traffic data" and also seek online access to information in the hands of an intermediary. The section provides:</p>	<p>For the purposes of this section,</p> <ul style="list-style-type: none"> • "computer contaminant" shall have the meaning assigned to it in Section 43;

(Continued)

Table 6.8 | (Continued)

<i>ITA 2008 Section</i>	<i>What it States</i>	<i>Comment</i>
	<ul style="list-style-type: none"> • The Central Government may, to enhance cybersecurity and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. • The intermediary or any person in-charge of the computer resource shall when called upon by the agency that has been authorized under subsection (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information. • The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed. • Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term that may extend to 3 years and shall also be liable to fine. 	<ul style="list-style-type: none"> • “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information. <p>Under this section, Government can force Cybercafes to follow safeguards specified and also demand online access if required.</p>

Note 1:

- The Karnataka Regulations for Cybercafes define a cybercafe as: *Any premises where the Cyber Cafe Owner/Network Service Provider provides the computer services including Internet access to the public.* Thus, in the Karnataka definition, *any Network Service Provider providing “Computer Services” may be called as the “Cyber Café.”*
- According to Tamil Nadu Regulations, a “Browsing Center” means and includes *any establishment by what so ever name called where the general public have an access to Internet in any of its forms, protocols either on payment or free of charges for any purpose including recreation or amusement.* It also says – *a browsing center shall be deemed to be a public place as defined under Sec-3 of Tamil Nadu City Police 1888.* Thus, in the TN definition, any Kiosks in say Airport or a Railway Station where free Internet access is given to public may also qualify as a cybercafe.
- The Tamil Nadu rules require registration of cybercafes and both impose responsibilities such as maintenance of visitor's register, verification of photo ID, etc.

Note 2:

- Additionally, three important sections have been added to the present Act according to which the government has the powers to intercept, monitor, block and collect traffic data. These sections impose certain responsibilities on the intermediaries and make non-compliance punishable. These regulations also apply to cybercafes.

Note 3:

- This section provides for blocking of websites in any case where prevention of a “cognizable offense” is intended. This can take care of blocking of websites that may host pornographic content, which is an offense under Sections 67, 67A and 67B of ITA 2008.

There is a serious concern that the powers under these sections (see Table 6.8) may be misused. To possibly prevent that, there is a need to set up an agency called *Netizen's Rights Commission* on the lines of the Human Rights Commission, which should have powers to receive complaints, investigate and recommend prosecution of abuse of the powers under Sections 69, 69A and 69B (refer to Table 6.7).

In the event any State Government would like to take up powers under these sections and also provide the benefits of the powers to the police, it would be advisable for the State Government to set up a "State Netizen's Rights Commission"^[15] and appoint the police to take up the scrutiny of the commission or set up a separate non-police agency such as a *State Cybersecurity Authority* and then vest the powers in such an authority. In the meantime, if the Central Government also notifies an agency for the purpose of exercising the authority under Sections 69, 69A and 69B and provides it with national jurisdiction across the country, then there may be a conflict of jurisdiction such as what we today have between the state police and the Central Bureau of Investigation (CBI).

The expectation is that the Indian Computer Emergency Team referred to under Section 70B of ITA 2008 may itself be designated as the agency of the Central Government with a national jurisdiction and Computer Emergency Response Team (CERT). (CERT India is the apex authority in India for cybersafety.) Considering that there are thousands of cybercafes all over India, in the event a central agency takes up the responsibility for monitoring cybercafes, there may be a need for an "All India Cyber Cafe Monitoring Authority" exclusively to meet the requirements of cybercafe regulations. Cybercafes must be now "more than ever" vigilant about security breaches since the protection they could claim under Section 79 has been largely made irrelevant as 79(2C) makes the protection subject to following of "due diligence."

With the security practices to be notified under Sections 69, 69A and 69B, the requirement of "due diligence" would be satisfied only if these security practices are maintained. It would, therefore, be necessary for cybercafes to undergo a *Cyber Law Compliance Audit* for fulfilling the specific requirements under these sections. In that case, if the government does not come out with any security practices guidelines for cybercafes, then also the due diligence requirements have to take into account the expectations under these sections. Either way there is a tough road ahead for cybercafes. At the same time, the police at the state level would be looking for clarification on whether they have the authority under Sections 69, 69A and 69B to regulate the cybercafes. They, however, continue to enjoy some powers under Section 80 with which they can still try to regulate cybercafes.

6.8.3 State Government Powers Impacted by the Amendments to the Indian IT Act

Indian States' legislative administration plays a crucial role in the implementation of the legislations along with the jurisdiction system and police. In this section we explain how the year 2008 amendments to the Indian Act have impacted the powers of the State Government in India. Around 45 amendments have been made to the original Act. It is said that with the passage of ITA 2008 (Amended ITA 2000), the role of State Governments in cyber regulations has undergone a significant change. Let us understand how this has happened.

Section 90 of the India ITA 2000 (Power of State Government to Make Rules) empowers State Government to make *rules* for the purpose of implementing the provisions of the Act assuming new meaning under ITA 2008. In ITA 2000, the section referred to powers required to be exercised under "Section 6" and Section 6 was in relation to E-Governance requirements such as filing of forms, granting of licenses, receipt of money, etc. There were not many other powers conferred on the State Government. Hence, *it could be interpreted that the powers of the state government were intended to be used only for giving effect to Section 6 and perhaps sections relating to the powers of the police.*

Although under ITA 2008, *no change has been made to Section 90*, the words “*...without prejudice to the generality of the foregoing power.*” used in Section 90(2) assume a greater meaning now since ITA 2008 envisages a lot more responsibilities and powers to State Government under the amended provisions. It is now no longer easy to restrict this section to only “Section 6” as it appeared appropriate in the earlier version. Now there are several more sections of ITA 2008 where State Government needs to exercise its powers.

Section 6A is regarding “delivery of services by service providers.” This section is one among the other sections under ITA 2008 that necessitates exercise of power by state. The provisions of Section 7A regarding *audit of E-documents* also apply to the State Governments and hence rules need to be framed for this purpose as well. Section 10 is another section under which rules are to be notified for *use of digital signatures or other approved forms of electronic signatures*, if any. Section 43A defines the liability of *body corporates* with regard to handling of “*sensitive personal information*” and makes a reference to “*reasonable security practices and procedures specified in any law for the time being in force.*” Owing to the definition of *law* that includes state laws and ordinances, it is possible for State Governments to define reasonable security practices for any class of users such as “*cybercafes*,” “*hotels*,” “*educational institutions*” or even “*households*.”

As for the *cybercafe regulations*, there is, however, a conflict in Section 67C where the Central Government alone has been vested with the powers to preserve and retain information in a particular manner and format for a specified duration. This is likely to have impact on cyberforensics investigation delays. Presently, some of the *State regulations on cybercafes* already specify such information and hence the State Governments need to review the present notifications and modify them in accordance with the ITA 2008.

Sections 69, 69A and 69B are of crucial importance because they provide powers to State Governments as well as to the Central Government regarding the following:

1. Appointing an officer or agency of the government specially authorized to intercept, monitor, decrypt, block access to any content, collect traffic data or information generated, transmitted, received or stored in any computer resource;
2. notifying procedures and safeguards for exercising the powers as indicated in the above paragraph;
3. defining the term *traffic data*.

Actually, the State Government can consider declaring any officer of the police department as an officer for the purpose of these sections. However, at different places, the Act has mentioned the “*powers of the police where relevant*” and has used the words “any officer” in Section 69 (Directions of Controller to a Subscriber to Extend Facilities to Decrypt Information) as well as in Sections 27, 28 and 46. The Act has also used the words “any agency of the government” in Sections 69A and 69B. This could perhaps be the intention of the legislature to not vest the powers (under Sections 69, 69A and 69B) with the police either at the state level or with CBI or the National Investigating Agency at the Central level. As a result of this, the State Government has to determine and notify which officer or agency would be entrusted with the responsibilities envisaged under these three sections (Sections 67, 69 and 90) and the procedures, safeguards, etc. to be associated with such appointment.

Under the modified Section 70, the appropriate government can declare any “*facility of critical information infrastructure*” as a “*protected system*.” The State Government has to frame rules and procedures to identify such systems, authorize appropriate persons in writing, how they are to be accessed, etc.

There is one more impact of ITA 2000: under Section 78 of ITA 2008, now *inspectors will be authorized to investigate cases* falling under the Act, instead of the DSPs. State governments, which had presently set up cybercrime police stations and cybercrime cells with statewide jurisdiction, need to review the system and consider if there is the need to declare more number of police stations as “*cybercrime police stations*.” This is especially so since the number of offenses falling under ITA 2008 are expected to outnumber those in the case of ITA 2000. Very importantly, under Section 79A, the Central Government may designate any

department, body or agency of the Central Government or State Government as “examiner of electronic evidence.” The State Government may have to, therefore, identify and recommend which state-level agency can be notified for this purpose. The net result is that State Governments will be exercising far more powers under the ITA 2008 than what was envisaged under ITA 2000. The powers also need to be accompanied by several definitions, procedures, safeguards, appointment of agencies, etc.

So a few key points to note are – under these amendments, the Indian Government is now allowed to “intercept messages” from mobile phones, computers and other communication devices to investigate any offense. Recall the recent furore in India about the RIM BlackBerry security matters that were flashed in the newspapers. It is not just about cognizable offense, the kind you witnessed in Mumbai 11/26 – it is about any offense. Also, to be able to effectively formulate a strategy for the State Governments, it requires to constitute an advisory body of experts which may be called the *Cyberlaw Advisory Group* so that detailed action plan can be drawn up for the systematic investigation of cyber-crime which is looming up as the new menace for the country. We can conclude that the ITA 2008 brings considerable amount of empowerment to the State Governments in India for the implementation of cybersecurity legislation.

6.8.4 Impact of IT Act Amendments on Information Technology Organizations

We discussed the powers that can be awarded to the State Governments in India. Now let us understand how the IT Act Amendments are going to impact the IT companies in India. There is a considerable amount of anxiety in the market today – IT and IT-enabled services (ITES) companies in India are keenly watching the amendments passed on by the Parliament in December 2008 to the 8-year-old ITA 2000. Some IT companies in India seem to be satisfied with the amendments. The impression is that ITA 2008 has, in a way, tried to address the demand for “data protection.” It has been India’s woo that there is no specific law on data protection. India is considered as one of the popular outsourcing destinations in the business process outsourcing (BPO) business zone. The reaction of the Indian IT and ITES companies is important from this perspective. Recall the discussion in Section 6.6 of this chapter.

The original ITA 2000 did provide that *data vandalism* would be *treated as an offense* under Section 66 of the Act with 3 year’s imprisonment and eligible for claiming compensation of up to ₹ 1 crore (₹ 1,00,00,000) under Section 43. However, there was no specific indication that this was a measure to protect data in the hands of BPOs. Many in the industry were of the opinion that there are no data protection laws in India. In authors’ opinion, this is a fairly valid point.

Although the government introduced a separate bill called *Personal Data Protection Act 2006*^[16] to meet this demand, the bill is still pending in the parliament and is likely to lapse. ITA 2008 has tried to address the demand of the IT industry by specifically introducing two sections, namely, *Section 43A* and *Section 72A*, which specify that they are *measures toward data protection*. This may make the Personal Data Protection Act 2006 redundant and superfluous at least to the extent of punishing breaches in data protection responsibilities of BPOs.

The fact that *India does not have a separate “Privacy Protection Law”* means there is no law so far to guarantee Indian Citizens’ right to protect their privacy except for the constitutional rights. “Privacy” has multiple dimensions: *informational, personal, communicational* and *territorial* and we are discussing here the “personal” dimension of privacy. The problem in this regard is that there is no definition of what is *sensitive personal information* and also there is no authority such as the *Data Commissioner* (unlike other countries, e.g., Canada) to whom complaints can be addressed by a data privacy victim. There is also no obligation for countries other than India to whom India sends sensitive personal information for

processing to have an acceptable data protection mechanism, etc.^[17] It is not adequate to simply declare compensation for offense related to data protection. These were already there in law and ITA 2008 may make it little more clarified and little more stringent. Now let us understand if the ITA 2008 has got provisions that can be considered cardinal for “privacy protection.” See sections of the ITA 2008 that are presented in Table 6.9.

Table 6.9 | ITA 2008 and Indian IT and ITES companies

<i>ITA 2008 Section and Title</i>	<i>What it States</i>	<i>Explanation for the Discussion in this Section</i>
Section 43A: Compensation for failure to protect data	Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.	<ol style="list-style-type: none"> 1. “Body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. 2. “Reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. 3. “Sensitive personal data or information” means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.
Section 72A: Punishment for Disclosure of information in breach of lawful contract	Save as otherwise provided in this Act or any other law for the time being in force <ul style="list-style-type: none"> • any person including an intermediary who • while providing services under the terms of lawful contract • has secured access to any material containing personal information about another person • with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain • discloses 	

(Continued)

Table 6.9 | (Continued)

<i>ITA 2008 Section and Title</i>	<i>What it States</i>	<i>Explanation for the Discussion in this Section</i>
Section 67C: Preservation and Retention of information by intermediaries	<ul style="list-style-type: none"> • <i>without the consent</i> of the person concerned, or in breach of a lawful contract • such material to any other person • shall be punished with imprisonment for a term which may extend to 3 years, or with a fine which may extend to 5 lakh rupees (₹ 500,000), or with both <p>The section states that:</p> <ul style="list-style-type: none"> • Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. • Any intermediary who intentionally or knowingly contravenes the provisions of subsection (1) shall be punished with an imprisonment for a term that may extend to 3 years and shall also be liable to fine. 	<p>An intermediary is also a member of the IT industry and the definition in Section 2(w) is wide enough to include many service providers. The definition states:</p> <ul style="list-style-type: none"> • “Intermediary” with regard to any particular electronic records, means • any person who on behalf of another person receives, stores or transmits that record or provides any service with regard to that record and • includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cybercafes.
Section 69: Powers to issue directions for interception or monitoring or decryption of any information through any computer resource	<ul style="list-style-type: none"> • Where the Central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of subsection (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or 	

(Continued)

Table 6.9 | (Continued)

<i>ITA 2008 Section and Title</i>	<i>What it States</i>	<i>Explanation for the Discussion in this Section</i>
Section 69A: <i>Power to issue directions for blocking for public access of any information through any computer resource</i>	<p>cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.</p> <ul style="list-style-type: none"> • The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed. • The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under subsection (1), extend all facilities and technical assistance to: <ul style="list-style-type: none"> • Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or • intercept or monitor or decrypt the information, as the case may be; or • provide information stored in computer resource. • The subscriber or intermediary or any person who fails to assist the agency referred to in subsection (3) shall be punished with an imprisonment for a term that may extend to 7 years and shall also be liable to fine. • Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient to do so in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offense relating to above, it may subject to the provisions of subsections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to 	

(Continued)

Table 6.9 | (Continued)

<i>ITA 2008 Section and Title</i>	<i>What it States</i>	<i>Explanation for the Discussion in this Section</i>
Section 69B: <i>Power to authorize to monitor and collect traffic data or information through any computer resource for Cybersecurity</i>	<p>be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.</p> <ul style="list-style-type: none"> • The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed. • The intermediary who fails to comply with the direction issued under subsection (1) shall be punished with an imprisonment for a term which may extend to 7 years and also be liable to fine. • The Central Government may, to enhance Cybersecurity and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. • The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under subsection (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information. • The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed. • Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to 3 years and shall also be liable to fine. 	<p>• “Computer Contaminant” shall have the meaning assigned to it in Section 43;</p> <p>• “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.</p>

Observations with Regard to Section 43A

There are a few observations on Section 43A of the IT Act.

1. The limit for compensation, which was ₹ 1 crore (₹ 1,00,00,000) under Section 43 of ITA 2000 has been removed. In other words, there is no upper limit for damages that can be claimed.
2. The government is expected to define *sensitive personal information* and it is the responsibility of *body corporates* to ensure that reasonable security practices are followed.
3. The definition of *reasonable security practice* is to be determined as explained below.
 - As defined in a mutual contract between the vendor and the processor of data or a data subject and the data processor.
 - As specified in any law for the time being in force.
 - To be specified by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Adherence to *contractual commitments* is a crucial aspect of service delivery. Therefore, the IT and ITES industry should first carefully examine the Service Level Agreements (SLAs) they have contractually committed to their customers. If the contract signed with the end customer or the document of understanding (DoU) signed with business intermediary does not mention the SLAs, then the service delivery organization should examine if there is any law directly impacting their IT Service Delivery activities. If neither is there, then the security practices to be specified by the government as a follow up of ITA 2000 would need to be followed. In the case of healthcare industry, in situations where SLA makes a mention of security practices as defined in Data Protection Act or the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (along with its recent revision through HITECH – *Health Information Technology for Economic and Clinical Health Act* to strengthen the Security Safe Guard Rule – see Box 6.18) or the Graham-Leach-Bliley Act (GLBA), Payment Card Industry–Data Security Standard (PCI-DSS), etc. will take precedence over any other security practice. For greater details about *Regulatory Compliance with International Standards*, readers are advised to refer to Ref. #6, Books, Further Reading.

Box 6.18

HIPAA-HITECH – Data Protection Implications for the Healthcare Industry

HIPAA stands for *Health Insurance Portability and Accountability Act* and HITECH Act stands for *Health Information Technology for Economic and Clinical Health Act*. They both are the governing acts in the US. They significantly impact service delivered by the healthcare industry worldwide.

Today, the way healthcare business operates worldwide, there are far more agencies (apart from just the patient and his physician or surgeon) involved with whom sensitive information about patient (known as "PHI" – Protected Health Information) may exchange hands. The regulation is aimed at protecting the PHI. There are "covered entities" who are bound by the HIPAA-HITECH to protect the PHI. Typical "covered entities" in the healthcare industries are: health plan owners (provides or pays the cost of medical care), healthcare clearinghouse (agencies who route electronic data between payers and providers, e.g., billing services), healthcare provider who transmits any health information in an electronic transaction (e.g., hospitals, physicians, public health departments, group homes, home health).

The HIPAA Security Rule applies to *electronic protected health information (EPAH)* which is individually identifiable in an electronic form:

1. An individual's past, present or future physical or mental health information;
2. an individual's provision of healthcare or
3. past, present or future payment for provision of healthcare

Box 6.18 HIPAA-HITECH – Data Protection . . . (Continued)

The primary objective of the security rule is to protect the confidentiality, integrity and availability of EPHI when it is stored, maintained or transmitted. Under HIPAA-HITECH, covered entities must maintain reasonable and appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of their EPHI against any reasonably anticipated risks.

There is also the *Privacy Rule in HIPAA*. It is with regard to the Protected Health Information (PHI). The HIPAA Privacy Rule applies covered entities that creates or receives health information. This rules covers the use and disclosure of health information about an individual in any format. A point to note is that the Privacy and Security Rule are NOT mutually exclusive. There are overlaps and interdependencies between the two rules. Both rules require appropriate and reasonable safeguards.

The IT and ITES industries may be satisfied with this clarification but they should now be concerned about the possibility of large liabilities to which they may be exposed as well as the need to follow compliance of international laws – for example, HIPAA-HITECH, GLBA, etc. mentioned previously. There is also a need to implement “Compliance Audits” to steer clear from the risk of being termed *negligent*. The judgment of what constitutes “negligence” would be left to the wisdom of the “Adjudicator” with regard to claims up to ₹ 5 crore (₹ 5,00,00,000) and a “Civil Judge” with regard to claims beyond ₹ 5 crore (₹ 5,00,00,000). The *unlimited liability* under Section 43A is good for a country that is a net exporter of data for processing. India being a predominant importer of data for processing has “unlimited liability”; however, this would be a hanging sword on the head of BPO company management. Any major calamity may result in a huge international liability that may wipe out the BPO in one single case of security breach. The wisdom of IT industry to force the government to impose a liability and responsibility on them through changes to ITA 2000 instead of voluntary code of ethics is perhaps questionable. In the IT and ITES sectors, there are many European countries with which Indian IT organizations are engaged for business delivery; such organizations are bound by the EU Clause (see Box 6.19).

Box 6.19

The EU Contract Clause – Understanding the Entities and Implications

Software businesses typically involve electronic processing of the data. In Europe, data privacy is considered to be citizens' right. For doing business with countries in the European Union (the EU), it is mandatory to sign the EU Contract Clause whenever transborder flow of information is involved; mainly personal data being imported from the EU countries. The entities to which the personal data belongs are called the *data subjects*.

The term *data subject* is very important in understanding the mandatory requirements of the EU Contract Clause. A data subject is an individual who is the subject of certain personal information. Data subjects can be multitude of people such as applicants, employees (current, former or retired), Multiple contract employees, expatriates, contractors, vendors/consultants, dependents and beneficiaries, retirement plan participants, prospective clients, consumers and customers, and investors. Data subjects could also be professionals related to the industry, patients, business contacts, service providers, agents, contractors and suppliers, market research participants, opinion leaders (influential scientists, academics, leading industry players, public officials, etc.) activists, visitors, etc.

As per EU definition “Personal data shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical,

Box 6.19 The EU Contract Clause – Understanding . . . (Continued)

physiological, mental, economic, cultural or social identity." The other important terms associated with personal data with the EU Contract gambit are: the *data controller* and the *data processor*. A *data controller* is commonly the natural or legal organization that alone or jointly with others determines the purposes and means of processing personal information. Determining purposes for which, and how personal information is, or is to be, processed may be the joint responsibility of two or more controllers; it does not need to be exclusive to just one. Determination is common where controllers share a pool of personal information, each processing independently of the other; for example, a number of companies accessing a centralized human resources database.

A *data processor* is commonly a natural or legal person that processes personal data on behalf of the controller. The origin of the EU Contract Clause is said to lie in the *EU Data Protection Directive* that compels member nations to enact national data protection laws harmonized with the principles of the directive (or more stringent) and to establish supervisory bodies to enforce the laws. It gives substance to and amplifies the CoE directive, especially, with regard to automated data processing.

The EU Contract Clauses have become important because under the *EU Data Protection Directive*, data cannot flow outside of EU if a contract is not in place in the exporting country. Both data exporter and data importer are liable to the data subject for *illegal data flows*. With regard to transborder flow of personal data, the following is important to note:

1. The EU Data Protection Directive requires the consent of the data subject to process their personal data in accordance with the purpose of collection. The data subject is usually an individual but can also be a corporate entity in some countries.
2. Personal data includes data such as E-Mail address, business contact details and other information attributable to an individual.
3. The data is collected and controlled under terms agreed with the data subject; for example, employment agreement, works council agreement, privacy policy, customer agreement or telephone consent.
4. The EU Data Protection Directive gives the data subject rights with regard to their data, including rights in relation to processing data offshore.
5. Local laws in Europe have implemented registration requirements for controllers and processors.
6. The data controller has responsibility to the data subject for handling of the data subject's data.
7. The data processor processes the data in accordance with the data controller's instructions.

Observations with Regard to Section 72A

Refer to Box 6.11 and key point *A Glimpse of Indian IT Act Amendment* under section "Section 72A of the Amended IT Act of India."

1. Under this section, disclosure "without consent" or "in breach of lawful contract" exposes a person including an "intermediary" to 3-year imprisonment. The offense is cognizable but bailable.
2. The disclosure should be either intentional or with knowledge that it may result in wrongful gain or loss (to somebody).
3. The subject material should contain "personal information." Note that unlike Section 43A, this section does not use the term *sensitive personal information*. Hence, "any personal information" can invoke this section if other conditions are satisfied. This applies only when the information is obtained in pursuance to a service offered.
4. Furthermore, under Section 85 (Offences by companies), the liabilities that fall on a company under this section will extend to any officer in-charge of business or director, etc. unless "due diligence" is proved.

There is one concern that arises from this section – it is regarding the use of the words such as "save as otherwise provided ... under any other law for the time being in force." This makes Section 72A subordinate to any such law, if it exists. This could be a source of nuisance litigation in the days to come. Although there

is no mention of a *grievance redressal mechanism* separately for victims of data security breaches in the form of *Data Commissioner*, the adjudication process with the Cyber Appellate Tribunal must be considered as adequate replacement. What is lacking, however, is a method of proactive regulation such as “compulsory registration of data processors” along with “de-registration as a means of penalizing a contravention.”

The need to enforce security norms for data exporters from India has not been specified. However, the extra territorial jurisdiction of this Act as per Section 75 may be interpreted as extending data protection obligations to any external party who under a contract takes up processing of data from India. There are some areas of concern for IT Companies – while the two sections (Sections 43A and 72A) directly impact IT Companies dealing with data processing, some of the following sections also have a significant impact on IT companies and could be source of irritation as well.

Observations with Regard to the EU Contract Clause

Refer to Box 6.19 to know more about the EU Contract Clause. Below are some observations with regard to the EU Contract Clause:

1. Indian data importers have some key obligations – contractual obligations, processing obligations, audit obligations as well as obligations with regard to onward transfers of personal data of data subjects to other countries with inadequate data protection.
2. European data exporter and Indian data importer are liable vis-à-vis data subject for their respective breaches.
3. Data exporter to do due diligence on Indian importer.
4. If data subject suffers damage because of Indian importer's wrong doing, data exporter who failed to use due diligence is also liable for damages.
5. Indian importer can be sued directly by a data subject. However, the data subject must first request data exporter to take action against Indian importer.
6. If data exporter fails to act within a reasonable period of time (1 month), data subject can sue Indian importer directly.

Observations with Regard to Section 67C

Here are some observations with regard to Section 67C of the IT Act:

1. We may note that this definition includes “Telecom Companies” such as AirTel or Reliance Infocomm or Tata Indicom. It includes Google, Rediff, Sify, Ebay.in, cybercafes, etc. It also includes many BPOs who operate as backoffice service providers, data centers, HR service providers, etc.
2. It is clear that a very large number of IT companies come under the scope of the Section 67C.
3. We are awaiting the notification regarding the time for which specified information needs to be preserved under this section. It could be 1 year in the minimum and 6–7 years at the outer end.

What is important to note is that any alleged non-compliance could expose the company and its executives to the penal provisions of this section as well as Section 65. As this is a “cognizable” offense, any “inspector” of police can now start questioning the CEO of a BPO if he is preserving the information, etc. Is it necessary for a police inspector to enter a BPO office and demand such information? Perhaps, this may initially happen with cybercafes. Later, it may happen at the offices of the ISPs and small portal owners. However, we never know if the larger organizations are immune to such intrusion. No discussion in ITA 2008 on privacy issues is complete without a reference to Sections 69, 69A and 69B that enable the government to exert a huge influence on the information security industry.

Although the powers which the government has gained through these three sections are justified in the context of the cybersecurity requirements, in the event appropriate safeguards are not enshrined in the rules and regulations, these three sections will become the most oppressive clauses of the new Act. To understand the reasons for coming to such conclusion, let us explore these three sections (Sections 69, 69A and 69B) in depth.

Observations with Regard to Section 69

We note the following observations with regard to Section 69 of the IT Act:

1. This section provides access to a designated agency of the Central or State Government to any information stored in any computer resource whether in a public place or in a private place, whether at home or at office with the excuse that it is required for prevention of or required for the investigation of any offense.
2. The power is not restricted to information in transit such as E-Mails but also other information that may be stored. This means that any police officer (or such other agency that may be designated under this section) under the excuse of investigating an offense (whether in the interest of national integrity or otherwise) can walk into any IT company and demand that he may intercept (access) information.
3. It is to be noted that non-cooperation by the company can result in imprisonment up to 7 years. The powers under Section 69 are oppressive enough to sit up and take notice. Sections 69A and 69B extend the powers further.

Observations with Regard to Sections 69A and 69B

The following observations with regard to Sections 69A and 69B are worth noting:

1. The two sections (refer to Table 6.9) extend the powers of interception and decryption in Section 69 to power to block access and power to demand “traffic data” from any person who is in possession of the relevant information. Refusal or non-cooperation is a cognizable offense.
2. Sections 69, 69A and 69B, therefore, provide what can be described as *brutal* powers to certain agencies.
3. It is not necessary that the designated agency under these sections should be the “police.” However, it is perhaps inevitable that police will either be directly designated as the “designated agency” under this section or will be the authority that will advise action under this section to any other agency otherwise designated. (As is presently the case with CERT-In with regard to blocking of websites with obscene content.) It is possible that the proposed “nodal agency” designated under Section 70B (that is called the Indian Computer Emergency Team which position may be occupied by the CERT-IN after due notification) may be entrusted with the responsibility of implementing the powers under Sections 69, 69A and 69B. However, the nodal agency may act on the basis of recommendations received from the police since it may not have direct capability for investigations.
4. Has any IT industry representative thought about the possible misuse of these sections and what would be the consequences thereof? If not, it is time to do this so that adequate safeguards can also be simultaneously introduced. It is time to think what should be such safeguards, how they should be implemented and which agency should monitor, etc.
5. To repeat my earlier comment, in the current scenario of threats prevailing in India, perhaps it is difficult not to accept such draconian laws as necessary. However, it is the responsibility of all of us to ensure that safeguards which are expected to be in place to prevent abuse of the powers under these three sections are adequate to ensure that the draconian powers are properly reigned and any abuse is adequately punished.
6. In particular, it is absolutely necessary that any agency, vested with powers under these three sections, should be answerable to a monitoring body which should have the powers to receive complaints from the public, conduct its own investigation even against police officers involved and also

- prosecute them as necessary. There should be no immunity given to such officials against being held accountable for breaches of propriety and law.
7. Such an agency should be like the “Human Rights Commission” and should be an independent body devoted to the welfare of the Netizens. It can be a new setup of a “Netizen Rights Commission” with the necessary powers. It should not simply be a judicial body with people who may not understand the technical issues involved. It must have representation of private persons of eminence who understand the technology issues and the human right violations that may arise therefrom.
 8. If there are legal hurdles to create such a commission, then it is suggested that a *Netizen’s Rights Advisory Board* is created in every state, which should receive complaints, investigate and give its recommendations. The recommendations may be taken up for implementation by the Human Rights Commission or the courts to provide justice to the aggrieved.
 9. In case appropriate safeguards and a monitoring mechanism are not immediately setup, there is a grave danger lurking ahead for IT companies and their executives who may become pawns in the hands of law enforcement officers who know where the law pinches and is able to tickle the sensitive spots in the IT industry.

6.9 Cybercrime and Punishment

In Section 6.2 there was discussion about the cybercrime legislation around the world. We also discussed the Indian scenario with regard to the ITA 2000 and its subsequent amendments known as the ITA 2008 that is not yet enforced. It is pending because certain rules are to be framed. While writing this section, there is a growing concern about the rise of cases committed against computers or against information on computers. The phenomenal rise in computer crime has caught attention around the world. The big question is whether cybercriminals can be punished and what types of punishments are in offering for them. In our opinion, in most countries around the world, existing laws are likely to be unenforceable against such crimes, given methods of crime adopted and tools used by cybercriminals (refer to Chapters 2 and 4, respectively). The possible lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to or destroy valuable information. Also refer to Chapters 9 and 10.

The situation is certainly not comfortable because although self-protection is essential, it is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. The ability to compete in the new digital economy will be much less for countries where legal protections are inadequate. As cybercrime crosses national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether they are sufficient to combat cybercrimes (see Chapter 1). Where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes.

Cybercriminals and cyberterrorists around the world seem to be undeterred by the prospect of arrest or prosecution as they lurk on the Net causing an omnipresent menace to the financial health of businesses, to the trust of their customers and as an emerging threat to nations’ security. Headlines of cyberattacks command our attention with increasing frequency. When it comes to punishment, it is the peculiar nature of cybercrime/computer crime (as compared to other forms of crime, i.e., non-computer crime) that presents the difficulty. Cybercrimes, which are the harmful acts committed from or against a computer or network, differ from most terrestrial crimes in four ways: (a) They are easy to learn how to commit, (b) they require few resources relative to the potential damage caused, (c) they can be committed in a jurisdiction without being physically present in it and (d) they are often not clearly illegal. The other problem that comes in way of punishing cybercriminals is that the laws of most countries do not clearly prohibit

cybercrimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their “virtual” counterparts. Often police officers may not realize (although there are constant efforts by government to educate the police departments on cybercrimes) how cybercrimes are different in nature compared to the traditional forms of crimes. For example, webpages such as the E-Commerce sites hit by widespread, distributed denial-of-service attacks may not be covered by outdated laws as protected forms of property.

In such a scenario, one may ask the following question: Why punishing the cybercriminals is so difficult? Part of the reason is that effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cybercriminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cybercrimes.

A key point to note is that the issue of cybercrime is closely related to information security. Although several countries, particularly in Europe and Asia, were found to have addressed a number of these broader information security factors, few countries have been able to demonstrate that adequate legal measures had been taken to ensure that perpetrators of cybercrime would be held accountable for their actions.

Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information, create a hostile environment from the standpoint of conducting E-Business within a country and across national boundaries. Inadequate legal protection of digital information can create barriers to its exchange and shunt the growth of E-Commerce. As E-Business expands globally, the need for strong and consistent means to protect networked information will grow. The overall picture is that substantial improvement is needed in information security. The year 2000 picture was that only a small fraction of countries needing substantial improvement indicated that progress was currently underway – refer to Fig. 6.4; it provides a categorization of the 52 countries surveyed. Figure 6.5 shows the details of laws that have been updated in each of the 19 countries with fully, substantially or partially updated laws in place.

When it comes to punishing the cybercriminals, one other problem is non-uniform treatment of crimes across the world: Crimes are not treated uniformly even in the countries that have got updated legislation for cybercrime and this creates another problem. We conclude about punishment to cybercriminals by summarizing the following key points:

1. **Reliance on terrestrial laws may not be a reliable approach:** Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cybercrimes. A majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court.
2. **Weak penalties limit deterrence:** The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects.
3. **Self-protection remains the first line of defense:** The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.
4. **A global patchwork of laws creates little certainty:** Little consensus exists among countries regarding exactly which crimes need to be legislated against. In the networked world, no island is an island. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cybercrime will be complicated.
5. **A model approach is needed:** Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of banning malicious

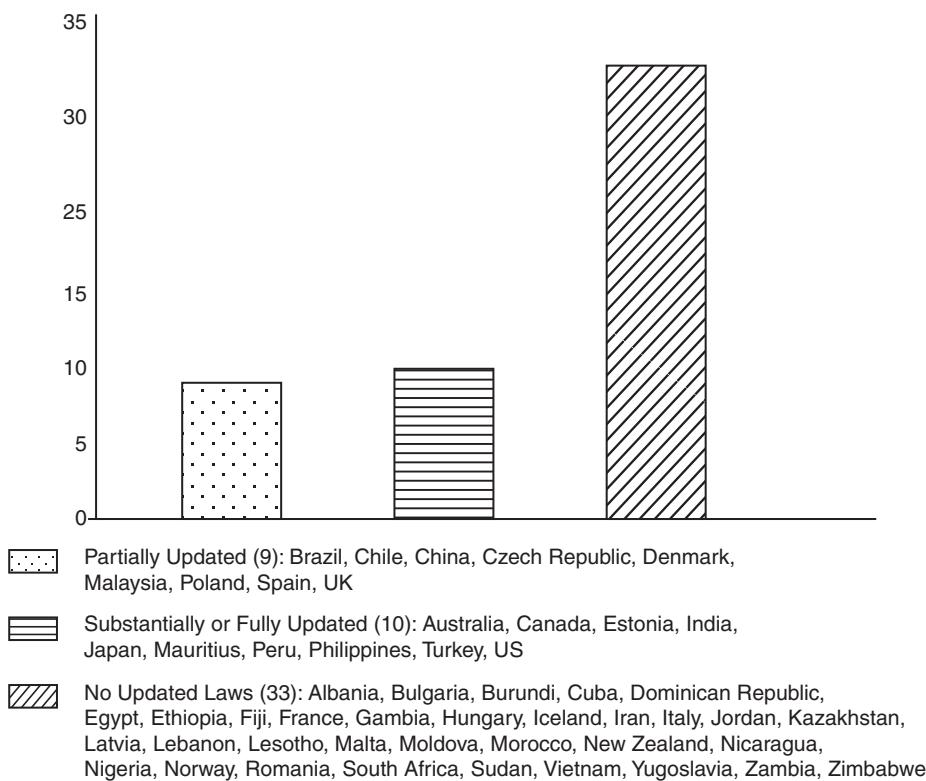


Figure 6.4 | Cybercrime laws: Extent of progress on updating.

computer-related acts in a timely manner to promote a secure environment for E-Commerce. But a few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated public–private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cybercrime havens.

6.10 Cyberlaw, Technology and Students: Indian Scenario

Recall the discussion in Section 6.5 (Challenges to Indian Law and Cybercrime Scenario in India) in which another dimension to the problem is discussed. India has a peculiar scenario given the current educational system. Most technology students have either nil or low exposure to law and most law students have only limited exposure to information technology. A computer science stream student in a college is taught how to develop programs that can automatically transmit data across the Internet riding on a TCP/IP packet, without alerting him on cybercrimes such as hacking or virus^[18] introduction. The topic of *secure coding* is not included in most syllabi. The Law students should be taught about Trade Marks and Copyrights without recognizing their implications on the electronic documents. As a result, neither the technologist nor the lawyer is trained in his formative years to understand cyberlaw.

Country	Network Crimes		Data Crimes			Related Crimes			Access Crimes	
	Network Interference	Network Sabotage	Data Interception	Data Modification	Data Theft	Aiding and Abetting Cybercrime	Computer-Related Forgery	Computer-Related Fraud	Unauthorized Access	Virus Dissemination
Australia	✓		✓	✓	✓			✓	✓	
Brazil		✓		✓		✓			✓	
Canada	✓	✓	✓	✓	✓			✓	✓	✓
Chile	✓	✓	✓	✓	✓					
China	✓			✓						✓
Czech Republic		✓		✓	✓			✓	✓	
Denmark	✓			✓				✓		
Estonia	✓	✓		✓	✓	✓		✓	✓	✓
India	✓	✓		✓	✓	✓		✓	✓	✓
Japan	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Malaysia				✓		✓		✓	✓	
Mauritius	✓	✓	✓	✓		✓	✓		✓	✓
Peru	✓	✓	✓	✓	✓			✓	✓	
Philippines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Poland	✓			✓	✓	✓				
Spain			✓	✓	✓	✓		✓		
Turkey	✓	✓		✓	✓	✓	✓	✓		✓
UK	✓	✓		✓		✓			✓	
US	✓	✓	✓	✓	✓	✓		✓	✓	✓

Figure 6.5 Countries with updated laws.**Notes:**

1. Network interference: Impeding or preventing access for others.
2. Network sabotage: Modification or destruction of a network or system.
3. Data interception: Interception of data in transmission.
4. Data modification: Alteration, destruction or erasing of data.
5. Data theft: Taking or copying data, regardless of whether it is protected by other laws, for example, copyright, privacy, etc.
6. Aiding and abetting cybercrime: Enabling the commission of a cybercrime.
7. Computer-related forgery: Alteration of data with intent to represent as authentic.
8. Computer-related fraud: Alteration of data with intent to derive economic benefit from its misrepresentation.
9. Unauthorized access: Hacking or cracking to gain access to a system or data.
10. Virus dissemination: Introduction of software damaging to systems or data.

Given the strides made by India in the IT and ITES as well as BPO domains, there is a strong need for techno-legal experts to demystify cyberlaw and make it possible for a large section of the society to take up study of cyberlaw. In future, Engineering, Commerce and Management colleges need to teach cyberlaw as an extension of computer science, commerce and management education, even while the law colleges try to extend their coverage of criminal laws and IPR laws to the cyberworld. To know more on IPR issues, readers may refer to Ref. #8, Books, Further Reading. Authors firmly believe that the advent of techno-legal

specialists will bring a change in the legal perspective in the country and we can expect fresh ideas to emerge to form building blocks for the development of cyber jurisprudence as a distinct field of study.

SUMMARY

IT is a vast and complex area. The growth in the number of Internet usage fuelled by easier availability of ICT, the widespread use of computers globally and the computer-friendly and tech-savvy younger generation are some of the factors that contribute to the cybercrime. There are many dimensions to cybersecurity; one is having the required *technical expertise* whereas another dimension is to have an *effective legal regime*. Yet another dimension is to have an *effective security infrastructure* that can use the technology and the law toward achieving the objective of securing the information assets of the country. In this chapter, we considered the second dimension. The world laws on cybercrimes embrace multiple dimensions of the issue as seen in the US, Europe, Asia-Pacific and Canadian position on the legal measures taken and being taken. In Indian law, cybercrime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act along with its recent amendment (the ITA 2008) provides the backbone for E-Governance and E-Commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. It is also said to provide certain authorities and powers to the State Governments in India. However, whether India has a strong Data Protection Act still remains a moot point. There is a general agreement though that there is a strong need to take into consideration the information security aspects of India. In the present global situation where cybercontrol mechanisms are important, we need to push cyberlaws. Cybercrimes are a new class of crimes in India, rapidly expanding due to extensive use of Internet. Getting the right lead and making the right interpretation are very important in solving a cybercrime.

Until recently, many IT professionals lacked awareness of and interest in the cybercrime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws would not quite fit for digital crimes committed, new laws need to catch up to the reality of what is happening. Furthermore, debates over privacy issues do hamper the ability of enforcement agents to gather the evidence needed to prosecute these new cases. There is also a certain amount of antipathy or at the least, distrust among the trio of most important players in any effective fight against cybercrime: law enforcement agencies, common people and computer professionals who need to be abreast of the technologies to prevent/detect cybercrime. Therefore, close cooperation between these entities is crucial if we are to control the cybercrime problem and make the Internet a safe “place” for its users. Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work and how to track down information on them. Common people need to be aware that they can be the target of cybercriminals. Each holds the key to defeating cybercriminals with their strong determination. IT professionals need good definitions of cybercrime to know when and what to report to police, but law enforcement agencies must have statutory definitions of specific crimes to charge a criminal with an offense. The first step in specifically defining individual cybercrimes is to sort all the Acts that can be considered cybercrimes into organized categories. Given the legal legislation enactment scenario in India as well as around the world, punishing the cybercriminals is not easy. However, the discussion in this chapter was aimed at making readers aware about the legal perspective on cybercrime.

REVIEW QUESTIONS

1. Explain the concept of “trust seal.” In your own understanding, along with additional research and discussion with lawyers, explain how it helps as a mitigation for frauds in E-Commerce.
2. What is the meaning of the term “cyberlaw”?
3. What do you understand by the salient features of the Indian IT Act?
4. In your view, do 2008 amendments to the Indian IT Act address the cybercrime issues that may emanate from cybercafe? Explain.
5. What, in your opinion, is required on the legal front to seek world harmony and convergence to bring about global measures to fight the cybercrime challenges? Explain what you think are the areas that need country cooperation across the globe.
6. Quote the Indian IT Act chapters that are relevant in the discussion of cybercrime and information security.
7. Is the current law (India as well as world) adequate to prevent unlawful access to computers? Why?
8. Under the Indian IT Act, is there a legal protection available for “personal data” and “sensitive personal data”? Explain how.
9. Does India have adequate legal means to punish cybercriminals? Explain your view point.
10. Do you feel the legal landscape around the world is integrated and harmonized? Why do you think so? Explain.
11. How does the legal legislation in the Asia-Pacific region compare to that in the European Union? Explain with at least three comparative points.
12. Do you think online child safety is an issue in India? Defend your answer with examples.
13. To prevent cybercrime, how do you think the APEC framework principles as well as the Fair Information Practices (FIPs) could be applied to design a commercial website?
14. Do you think the EU legal framework is strong enough to prevent cybercrimes? Explain why you think so.
15. Do “electronic records” have the admissibility into Indian Courts? Explain why.
16. Describe the strengths and limitations of the Indian ITA 2000. Do you think the limitations/weakness are overcome by the 2008 amendments to the Act? What would be the impact, in your view, of not addressing the current weaknesses in the Indian IT Act?
17. Describe the specific challenges that exist in India with regard to the law and cybercrime scenario in India.
18. In your view, is the issue of “digital certificates” adequately addressed in the Indian IT Act? Explain why.
19. Under the current Indian law (the IT Act) what are the implications for “Certifying Authorities”?
20. Explain the powers endowed upon the State Government as the result of amendments to the Indian IT Act. Do you think that with the amendment to the Indian IT Act, the State Governments in India are better off in investigating cybercrimes emanating from the use of cybercafes? Explain why.
21. How do you think the matter of “Data Protection Law in India” stand with the introduction of the ITA 2008? Do you feel that foreign companies planning to send outsourcing work to India should feel happy with the current developments? Explain your view point.
22. What are your views on punishments for cybercriminals? Is it possible to punish them? If not, then what do you think are the deterring factors in India as well as globally?

REFERENCES

- [1] To understand the *Privacy Threats from Social Networking Sites*, readers should visit:
A good write up on Indian Laws for use of Social Networking Sites can be downloaded by visiting:
<http://www.indiasafe.com/image/PDF-sep-08/social-networking.pdf> (12 July 2009).
A paper of Privacy and Social Networks is available at the link mentioned below
<http://www.w3.org/2008/09/msnwspapers/tilt.pdf> (10 May 2009).
ENISA Guidance – Security Issues and Recommendations for Online Social Networks, is available at:
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf (10 August 2009).
Another Paper on *Privacy Threats from Social Networking Sites* can be downloaded from
http://www.digiwebbs.com/research_paper.pdf (14 April 2009).
Another site worth visiting about Privacy Issues in Social Networking site is <http://privacyinsocialnetworksites.wordpress.com/> (3 September 2009).
- [2] For the *Indian ITA 2000*, refer to the URL at:
<http://www.legalserviceindia.com/cyber/itact.html> (2 May 2009).
- [3] <http://www.naavi.org/importantlaws/itbill2000/preamble.htm> (29 December 2009).
- [4] The European Union and the EU Member Countries can be visited at:
http://en.wikipedia.org/wiki/European_Union (20 July 2009).
http://en.wikipedia.org/wiki/European_Union_member_state (20 July 2009).
<http://geography.about.com/od/lists/a/eumembers.htm> (20 July 2009).
http://en.wikipedia.org/wiki/European_Union_Monitoring_Mission (20 July 2009)
- [5] <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf> (29 December 2009).
- [6] To know more about the country-wise position on data protection laws, visit: <http://www.guardianedge.com/resources/data-protection.php> (20 July 2008).
- [7] COPPA is Children's Online Privacy Protection Act – the FAQs are available at: <http://www.ftc.gov/privacy/coppafaqs.shtm> (18 August 2009).
- [8] A thematic paper (presented at Rio de Janeiro, Brazil on November 25–28, 2008) on *Child Pornography and Sexual Exploitation of Children Online* can be read at:
http://www.meldpunkt-kinderporno.nl/files/Biblio/Thematic%20Paper_ICTPsy_ENG.pdf.
- [9] For *Council of Europe's Convention on Cyber Crime*, visit:
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (11 August 2009).
http://www.coe.int/t/dc/files/themes/cyber-crime/default_EN.asp (11 August 2009).
Computer Crime & Intellectual Property Section, United States Department of Justice can be visited at:
<http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm> (11 August 2009).
- [10] For Organization for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*, visit:
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1,00.html (20 August 2009).
<http://www.oecdbookshop.org/oecd/display.asp?K=5LMQCR2JGG0T&DS=OECD-Guidelines-on-the-Protection-of-Privacy-and-Transborder-Flows-of-Personal-Data> (20 August 2009).
- [11] For the *Indian Penal Code* and its Amendment Bill, visit:
http://rajyasabha.nic.in/bills-ls-rs/2000/XXXVIII_2000.pdf (1 January 2010).

<http://chddistrictcourts.gov.in/THE%20INDIAN%20PENAL%20CODE.pdf> (5 January 2010).

<http://www.netlawman.co.in/acts/indian-penal-code-1860.php> (5 January 2010).

- [12] Visit the following links for the *Indian Evidence Act* at:

<http://chddistrictcourts.gov.in/THE%20INDIAN%20EVIDENCE%20ACT.pdf> (29 December 2009).

<http://www.indianrailways.gov.in/RPF/Files/law/BareActs/Evidenceact.doc> (29 December 2009).

http://en.wikipedia.org/wiki/Indian_Evidence_Act (29 December 2009).

- [13] For *Bankers' Books Evidence Act* of 1891, visit:

<http://www.indianrailways.gov.in/RPF/files/law/BareActs/Bankbookact.doc> (15 August 2009).

<http://indiocode.nic.in/rspaging.asp?fnm=189118> (15 August 2009).

<http://www.vakilno1.com/bareacts/Laws/The-Bankers-Book-Evidence-Act-1891.htm> (15 August 2009).

- [14] Visit the following links for the *Reserve Bank of India Act* 1934 at:

<http://www.helplinelaw.com/docs/THE%20RESERVE%20BANK%20OF%20>

[INDIA%20ACT,%201934/CHAPTER%20V%20PENALTIES](#) (1 August 2009).

http://en.wikipedia.org/wiki/Reserve_Bank_of_India (1 August 2009).

- [15] The article about *National Netizen's Rights Commission* can be read at:

<http://www.merinews.com/catFull.jsp?articleID=154783> (13 August 2009).

<http://www.bloggernews.net/119210> (13 August 2009).

- [16] Regarding the *Personal Data Protection Act of India*, visit:

<http://www.legalserviceindia.com/article/137-Data-Protection-Law-in-India.html> (11 August 2009).

<http://www.legalserviceindia.com/article/1368-Data-Protection-Law-In-India.html> (11 August 2009).

<http://www.indlawnews.com/display.aspx?4530> (11 August 2009).

- [17] Refer to the following link for an Interactive Map of *Data Security Breach Disclosure Laws in the United States* presented by GuardianEdge Technologies and powered by Google Maps:
<http://www.guardianedge.com/resources/breach-disclosure.php> (23 August 2009).

- [18] For an explanation about "viruses" visit: <http://cybercrime.planetindia.net/viruses.htm> (22 August 2009).

FURTHER READING

Additional Useful Web References

- For Cyber Crime Investigation Cell and contact E-Mail, visit: <http://www.cybercellmumbai.com/contact-us> (9 August 2009).
- For the list of cybercrime police station in different states in India, with the names of officers in charge, you can visit: http://www.naavi.org/cl_editorial_04/cyber_Crime_ps.htm (8 May 2009).
- To know about a 720 pages book with comprehensive coverage on cyberlaws in India, readers can

visit: http://www.naavi.org/archives/archive_edit_feb_28_04.htm (12 July 2009).

- The following link has very useful information about Internet censorship: law and policy around the world: <http://www.efa.org.au/Issues/Censor/cens3.html> (25 July 2009).

- Internet Security and Computer Crime, A Guide to Selected Government Information, available at WIU's Government Publications Library, can be accessed at: <http://www.wiu.edu/library/gov-pubs/guides/internet.htm> (1 June 2009).

6. Visit the following URL for *The Electronic Commerce Support Act – 1998*; it is an Act to amend various Central Acts to facilitate electronic commerce: http://www.indianembassy.org/policy/Commerce/eCommerce/eCommerce_support_act_1998.htm (20 April 2009).
7. The following link is about Child Online Safety discussion at the Internet Governance Forum (IGF): <http://www.intgovforum.org/cms/index.php/component/chronocontact/?chronoformname=WSProposals2009View&wspid=288> (19 February 2010).
8. To understand digital signatures, visit: http://asclonline.com/images/d/d4/Simple_Guide_to_Digital_Signatures.pdf (15 April 2009).
9. The following links can be visited for the *Indian IT Act 2000* at:
 - <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN010239.pdf> (22 February 2009).
 - <http://vlex.in/vid/the-information-technology-act-29635830> (21 July 2009).
 - <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf> (17 December 2008).
 - http://www.itwire.com/index2.php?option=com_content&do_pdf=1&id=4957 (31 July 2008).
10. The following links can be visited to understand about the amendments to the Indian IT Act 2000 that were made toward the end of year 2008, that is, the ITA 2008.
 - <http://www.cyberlaws.net/itamendments/index1.htm> (21 July 2009).
 - <http://www.alertindian.com/?q=node/23> (21 July 2009).
 - <http://www.alertindian.com/?q=node/33> (21 July 2009).
11. For a good debate as to whether India needs a Data Protection Legislation, refer to the following URL: <http://www.algindia.com/publication/article3200.pdf> (21 July 2009).
12. Following are some good links on electronic commerce for those who are not familiar with

E-Commerce (building blocks of E-Commerce are explained in this paper):

http://www.cs.berkeley.edu/~tygar/papers/Building_blocks_atomicity_e-comm.pdf (12 May 2008).

For understanding the basics of E-Commerce, visit:

<http://thestar.com.my/maritime/news/2000/2/27edi1.html> (21 July 2009).

http://www.nvcc.edu/home/kvu/eCommerce_a.pdf (21 July 2009).

An E-Commerce online tutorial is available at:

<http://www.webdevelopersjournal.com/columns/eCommerce1.html> (15 March 2009).

Internet Commerce basics are explained at:

<http://www.electronicmarkets.org/issues/volume-8/volume-8-issue-1/internetcommerce-basics0.pdf> (10 September 2008).

13. For explanation of *digital signatures* in easy and non-technical language, the following site can be visited at: <http://www.youdzone.com/signature.html> (28 July 2009).
14. Visit the following URL to read the article *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure*: <http://www.schneier.com/paper-pki.html> (3 August 2009).
15. To understand about *Use of S/MIME as a security measure for online communication*, visit:
 - <http://www.elock.com/S-MIME-article2.html> (1 August 2009).
16. To understand about *Privacy-Enhanced Mail (PEM)*, visit: http://www.cs.umbc.edu/~woodcock/cpsc_482/proj1/pem.html (1 August 2009).
17. Visit the following excellent site on *Global Laws & Legislations* (on this site, you can get the links to the cybercrime laws in countries around the world):
 - <http://www.ccmostwanted.com/LL/global.htm> (5 September 2009).
18. For *Comments of Naavi on the Amendments Proposed to ITA-2000 vide ITAA 2008*, refer to the following link: http://www.naavi.org/cl_editorial_08/edit_dec_28_itaa_analysis_5_overview.htm (13 August 2009).

19. Canadian Anti-Spam Laws – for full text of bill S-220, an Act respecting commercial electronic messages, visit: http://www2.parl.gc.ca/content/Senate/Bills/402/public/S-220/S-220_1/S-220_text-e.htm (19 August 2009).
20. For discussion blogs on Canada's proposed Anti-Spam Legislation (Bill S-220; previously S-202), visit: http://groups.google.ch/group/news.admin.net-abuse.email/browse_thread/thread/e0759ea7928a14e2 (18 August 2009).
21. Also see the following link to read about Canada's fight against spammers: <http://www.spamfighter.com/News-11925-Canada-Prepares-to-Fight-against-Spammers-Anti-Spam-Bill-in-Senate.htm> (15 August 2009).
22. Visit the important link for European Committee on Crime Problems (CDPC) Committee of Experts on Crime in Cyber-Space (PC-CY) Draft Convention on Cyber-crime (Draft No. 22 REV) at: <http://www.cyber-rights.org/documents/coe22.htm> (22 August 2009).
23. For the South African legislation on cybercrime and specifics of Spam specified in their ECT Act, refer to Section 2 on Pg 9 of the document that is available in the following link: <http://www2.law.uu.nl/priv/AIDC/PDF%20files/IIIB2/IIIB2%20-%20South%20Africa.pdf> (21 August 2009).
24. To read the story about Management Cyber-gang stealing £12.8m from South African Government, refer to the following link: <http://www.computerweekly.com/Articles/2008/06/11/231018/cybergang-steals-12.8m-from-south-african-government.htm> (11 July 2009).
25. To understand how Spam works, visit: <http://computer.howstuffworks.com/spam.htm/printable> (30 August 2009).
26. Another view on Spam is available at the following link: <http://www.pgts.com.au/pgtsj/pgtsj0309a.html> (12 August 2009).
27. To understand about the *Fight against Spam*, refer to the following link: http://www.openmag.com/features/Vol_39/spam/spam.htm (23 August 2009).
28. A contrary view that Spam should not be legislated is available at: <http://www.progoth.com/spam/termpaper.html> (20 August 2009).
29. At the following links, there are articles about India's approach to fight against cybercrimes: <http://www.goarticles.com/cgi-bin/show.cgi?C=3128083> (19 August 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Appendix AG in the CD explains WebTrust – Seal of Approval – the Criteria for Extended Validation Certificates, “EV Certificates”), Wiley India Pvt. Ltd., New Delhi.
2. Ibid, Chapters 29, 30, 31 and 32.
3. Ibid, Chapter 14 (Intrusion Detection for Securing the Networks).
4. Ibid, Chapter 29 (Privacy – Fundamental Concepts and Principles).
5. Ibid, Chapter 13 (Cryptography and Encryption).
6. Ibid, Chapter 27 (Laws and Legal Frameworks for Information Security).
7. Ibid, Chapter 13 (Section 13.5 Digital Signatures – A Method for Information Security and Section 13.6 Cryptographic Algorithms).
8. Ibid, Chapter 38 (Ethical Issues and Intellectual Property Concerns for Information Security Professionals).
9. Broadhurst, R. and Grbosky, P. (2005) Cyber crime in India – the legal Approach, *Cyber-Crime: The Challenge in Asia*, Hong Kong University Press, Hong Kong.
10. Oberoi, S.. *E-Security and You*, Tata McGraw Hill, Delhi.
11. Kieran, B. (2000) *Small Business Solutions E-Commerce*, Microsoft Press, USA.

12. Shurety, S. (2000) *e-business with Net.Commerce*, IBM Press.
13. Kosiur, D. (1997) *Understanding Electronic Commerce*, Microsoft Press, USA.
14. Laudon, K.C. and Traver, C.G. (2003), *E-commerce: Business, Technology, Society*, Pearson Education, Singapore.
15. Kalakota, R. and Whinston, A.B. (1999) *Frontiers of Electronic Commerce*, Pearson Education, New Delhi.
16. Amor, D. (2000) *The E-business (R) Evolution*, Pearson Education.
17. Shaw, M, Blanning, R. Strader, T., and Whinston, A. (2003), *Handbook of Electronic Commerce*, Springer, USA.
18. Broadhurst, R.G. and Grabosky, P.N. (2005) *Cyber-crime: the Challenge in Asia* Hong Kong University Press, Hong Kong.

Articles and Research Papers

1. *Computer Crime and Computer Fraud*, University of Maryland, Department of Criminology and Criminal Justice, Fall, 2004 can be accessed at: http://www.montgomerycountymd.gov/content/CJCC/pdf/computer_crime_study.pdf (1 January 2009).
2. A paper by *Crime Data Mining: An Overview and Case Studies* by Hsinchun Chen, Wingyan Chung, Yi Qin, Michael Chau, Jennifer Jie Xu, Gang Wang, Rong Zheng, Homa Atabakhsh from Artificial Intelligence Lab, Department of Management Information Systems, University of Arizona, Tucson, AZ 85721, USA can be read at: <http://www.fbe.hku.hk/~mchau/papers/CrimeDataMining.pdf> (1 July 2009).
3. For *CRS Report for Congress, Cybercrime: The Council of Europe Convention* by Kristin Archick, Specialist in European Affairs Foreign Affairs, Defense and Trade Division, refer to the following links:
<http://fpc.state.gov/documents/organization/36076.pdf> (12 April 2008).
<http://fpc.state.gov/documents/organization/58265.pdf> (12 April 2008).
4. For cybercrime outlook in the Middle East, visit: <http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf> (5 January 2009).
5. Refer to paper on *Cyber Insurance* by Rainer Böhme, Technische Universität Dresden, Institute for System Architecture 01062 Dresden, Germany in the following link: <http://infosecon.net/workshop/pdf/15.pdf> (19 October 2008).
6. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions about *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* is available at: <http://www.usdoj.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf> (21 April 2009).
7. CRS Report for Congress about *Terrorist Capabilities for Cyberattack: Overview and Policy Issues* by John Rollins, Specialist in Terrorism and International Crime Foreign Affairs, Defense, and Trade Division and Clay Wilson, Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division (Updated January 22, 2007) is available at: <http://www.fas.org/sgp/crs/terror/RL33123.pdf> (3 July 2009).
8. A presentation based on the Proceedings of WSIS Thematic Meeting on Cyber security, about harmonizing National Legal Approaches on Cyber crime is available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf (3 March 2009).
9. For documents and links concerning digital evidence, visit: <http://www.khodges.com/digitalphoto/offtopiclinks.htm> (7 July 2009).

- 10.** *The Threat of the Cybercrime Act 2001 to Australian IT Professionals*, a paper by Nelson Chan and Simon Coronel from Department of Computer Science and Software Engineering, The University of Melbourne and Yik Chiat Ong from Faculty of Law, The University of Melbourne. –The paper can be read at: <http://www.cs.berkeley.edu/~benr/publications/auscc03/papers/chan-auscc03.pdf> (12 August 2010).
- 11.** UNCITRAL stands for United Nation's Commission on Internet Trade Law. Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998 United Nations. The UNCITRAL document (refer to Section 6.3) can be visited at: [http://www.genghinieassociati.it/acrobat/it%20security/Leggi/UNCITRAL%20Model%20Law%20on%20Electronic%20Commerce%20\(English\).PDF](http://www.genghinieassociati.it/acrobat/it%20security/Leggi/UNCITRAL%20Model%20Law%20on%20Electronic%20Commerce%20(English).PDF) (16 August 2009).

The Appendices that serve as extended material for the topic addressed in this chapter are: A, B, D, F, J, M, O, P, Q, U, V. These are provided in companion CD.

Note: Laws and Legal/Legislative Provisions mentioned in this chapter are as they stood at the time of writing the texts in the chapter. It is readers' responsibility to refer to the updated documents to know the latest position. For the Indian IT Act, readers should refer to the books available in the market, for example, "BARE ACT."

7

Understanding Computer Forensics

Learning Objectives

After reading this chapter, you will able to:

- Understand the fundamental concepts in cyberforensics.
 - Understand the meaning of the term “cyberforensics and the need for cyberforensics.”
 - Learn what “digital evidence” means along with the base term “forensics science.”
 - Get an overview of cardinal rules of computer forensics.
 - Learn how cyberforensics is used in cybercrime investigations.
 - Understand the legal requirements for cyberforensics and compliance aspects of cyberforensics.
 - Get an overview of the role of forensics experts.
 - Understand the “data privacy issues” involved in cyberforensics.
 - Learn about forensic auditing.
 - Learn about cyberforensic tool available in the market.
 - Understand the challenges faced in cyberforensics.
-

7.1 Introduction

The purpose of this chapter is to address the other side of crime, that is, use of forensic techniques in the investigation of cybercrimes. “Cyberforensics” is a very large domain and addressing it in a single chapter is indeed a challenge. Complex technical aspects involved in digital forensics/computer forensics are not possible to cover in a single chapter. Therefore, this chapter is aimed at only providing a broad understanding about cyberforensics.

The term “chain of custody” has a recurring mention in this chapter because it is a central concept in forensics. We have provided a large number of information resources including several video clips on digital forensics investigation (some demonstrations too), reviews of forensics tools as well as interviews with experts. We recommend readers to visit those links in Video Clips, Further Reading. The discussion in this chapter will serve as background for Chapter 8 where hand-held forensics is addressed. The terms “cyberforensics,” “digital forensics” and “computer forensics” are used interchangeably. Definitions of these terms are provided.

Cyberforensics plays a key role in investigation of cybercrime. “Evidence” in the case of “cyberoffenses” is extremely important from legal perspective. There are legal aspects involved in the investigation as well as handling of the digital forensics evidence. Only the technically trained and experienced experts should be involved in the forensics activities.

The requirements for setting up a digital forensics laboratory are explained in Section 7.11. Toward the end, a ready reckoner of cyberforensics tools is provided in a tabular form for readers' convenience (Tables 7.9, 7.10 and 7.11). Considering the widespread use of hand-held devices [personal digital assistants (PDAs), mobile phones and all its varieties as well as the iPods, etc.], we have addressed the forensics of hand-held devices in the next chapter. Some special topics such as "use of data mining in cyberforensics," "forensics auditing" and "antiforensics" are also discussed in this chapter. Case studies on digital forensics investigations are presented in Chapter 11 (in CD). With this background, let us proceed to understand the historical background.

7.2 Historical Background of Cyberforensics

The different types of cybercrimes are explained in Chapter 1. Computer is either the subject or the object of cybercrimes or is used as a tool to commit a cybercrime. The earliest recorded computer crimes occurred in 1969 and 1970 when student protestors burned computers at various universities. Around the same time, people were discovering methods for gaining unauthorized access to large-time shared computers. Computer intrusion and fraud committed with the help of computers were the first crimes to be widely recognized as a new type of crime.



The Florida Computer Crimes Act was the first computer crime law to address computer fraud and intrusion. It was enacted in Florida in 1978. [Mentioned in Chapter 6, (Box 6.6 in Chapter 6).]

The application of computer for investigating computer-based crime has led to development of a new field called *computer forensics*. Sometimes, computer forensics is also referred to as "digital forensics." Computer forensics/digital forensics has existed for as long as people have stored data inside computers.



"Forensics evidence" is important in the investigation of cybercrimes.

Discussion on the legal side of cybercrime (see Chapter 6) serves as a link to this chapter through the term "evidence," "digital evidence" in particular. Basically, computer forensics experts need digital evidence in cases involving data acquisition, preservation, recovery, analysis and reporting, intellectual property theft, computer misuse (recall the discussion in Chapter 6 about the Indian IT Act – Tables 6.6, 6.7 and 6.8), corporate policy violation, mobile device (PDA, cell phone) data acquisition and analysis, malicious software/application, system intrusion and compromise, encrypted, deleted and hidden files recovery, pornography, confidential information leakage, etc.

Computer forensics is still a relatively new discipline in the domain of computer security. It is a rapidly growing discipline and a fast growing profession as well as business. The focus of computer forensics is to find out digital evidence – such evidence required to establish whether or not a fraud or a crime has been conducted. There is a difference between computer security and computer forensics. Although "computer forensics" is often associated with "computer security," the two are different.



Computer forensics is primarily concerned with the systematic “identification,” “acquisition,” “preservation” and “analysis” of digital evidence, typically after an unauthorized access to computer or unauthorized use of computer has taken place; while the main focus of “computer security” is the prevention of unauthorized access to computer systems as well as maintaining “confidentiality,” “integrity” and “availability” of computer systems.

Information security aspects are explained in detail in Ref. #14, Books, Further Reading. Thus, the goal of computer forensics is to perform a structured investigation on a digital system. For those who are reading this chapter directly before visiting Chapter 1, computer crime is any criminal offense, activity or issue that involves computers.



There are two categories of computer crime: one is the criminal activity that involves using a computer to commit a crime, and the other is a criminal activity that has a computer as a target.

Information security experts consider “cyberlaw compliance” as one of the many aspects of “techno-legal information security.” They advise organizations to formulate an appropriate plan of action to comply with cyberlaws as a part of the IS practice. This association of cyberlaw into the information security domain has gained additional importance due to some amendments that have been made to ITA 2000. Typical types of data requested for a digital forensics examination by the law enforcement agencies include: investigation into electronic mail (E-Mail) usage, website history, cell phone usage, cellular and Voice over Internet Protocol (VoIP) phone usage, file activity history, file creation or deletion, chat history, account login/logout records and more. Therefore, it becomes necessary to address the legal issues involved in cyberforensics. This is addressed in Section 7.16.2. Tables 7.9, 7.10 and 7.11 provide the list of forensic tools available in the market. URLs are also provided in Refs. #15, #16, #17 and #18, Additional Useful Web References, Further Reading with information about various laws/statutes pertaining to cybercrime. This information would be particularly useful for cyberlaw students.



Forensics means a “characteristic of evidence” that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence level).

In precise terms, “forensics science” is the application of science to law and it is ultimately defined by use in court. Forensics science is the application of physical sciences to law in search for truth in civil, criminal and social behavioral matters to the end that injustice shall not be done to any member of society. An alternative definition for digital forensics science is:

the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.



The goal of digital forensics is to determine the “evidential value” of crime scene and related evidence.

The roles and contributions of the digital forensics/computer forensics experts are almost parallel to those involved as forensics scientists in other crimes, namely, analysis of evidence, provision of expert testimony, furnishing training in the proper recognition, and collection and preservation of the evidence. Now, let us understand the term “digital forensics science.”

7.3 Digital Forensics Science

Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence. There is a number of slightly varying definitions. The term *computer forensics*, however, is generally considered to be related to the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is *magnetically stored or encoded*. The objective of “cyberforensics” is to provide digital evidence of a specific or general activity. Following are two more definitions worth considering:

1. **Computer forensics:** It is the *lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information* that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations. In other words, it is the collection of techniques and tools used to find evidence in a computer.
2. **Digital forensics:** It is the use of *scientifically derived and proven methods* toward the *preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence* derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Box 7.1 COFEE Time!



Computer Online Forensics Evidence Extractor (COFEE) is a USB thumb-drive gadget onto which Microsoft have loaded 150+ “commands” that can, among other things, decrypt passwords, display Internet activity and uncover all data stored on the computer. This interestingly named tool was developed by Anthony Fung, a former Hong Kong police officer now working as a senior investigator on Microsoft’s Internet Safety Enforcement Team. Microsoft’s intent behind creation of COFEE has been exclusively for use by law enforcement agencies. It is believed that while creating the design of this tool, Microsoft perhaps did not take into consideration the feedback about problems faced by law enforcement agencies worldwide. During their ongoing fights against a variety of cybercrimes, law enforcement agencies around the world face some common challenges.

Box 7.1 COFEE . . . (Continued)

Law enforcement professionals need to capture critical evidence on a computer at the scene of an investigation before the evidence is powered down and removed for forensics analysis. Digital evidences, when "live" (e.g., active system processes and network data), must be handled with care because the "live" evidence is volatile. There is always the risk of "volatile evidence" getting lost when the computer is turned off. Therefore, the challenge is how does an officer on the scene effectively do this if he/she is not a trained computer forensics expert?

COFEE helps the law enforcement agencies even when there are no on-the-scene computer forensics capabilities. It enables them to collect live "volatile evidence" more easily, reliably and cost-effectively. Even a law enforcement officer with minimal computer experience, once he/she is taken through the tool tutorial, can use a preconfigured COFEE device. The officer can take advantage of the same common digital forensics tools as used by experts to gather volatile evidence that can prove critical for the investigation. The officer can undertake investigation tasks by simply inserting a USB device into the computer.

On-the-scene, agents can run more than 150 commands on a live computer system. COFEE tool also provides reports in simple format that are easy for later interpretation. These reports can be used by experts and can also be used as supportive evidence for subsequent investigation and prosecution. The COFEE tool and its underlying framework can be tailored to effectively meet the needs of a particular investigation, that is, it can be fully customized. On the lighter side, one wonders if there will also be Total Evidence Analyzer (TEA) soon.

More information on the COFEE^[1] tool can be obtained by visiting the links provided in References. We have provided a link in Ref. #2, Video Clips, Further Reading, where a computer forensics expert explains how digital evidence is seized as part of forensics investigation.

It is difficult to provide a precise definition of "digital evidence" because the evidence is recovered from devices that are not traditionally considered to be computers. Some researchers prefer to expand the definition by including the "collection" and "examination" of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices. In general, the role of digital forensics is to:

1. Uncover and document evidence and leads.
2. Corroborate evidence discovered in other ways (E-Discovery – see Box 7.3).
3. Assist in showing a pattern of events (data mining has an application here).
4. Connect attack and victim computers (Locard's Exchange Principle – see Box 7.5).
5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.
6. Extract data that may be hidden, deleted or otherwise not directly available.

The typical scenarios involved are:

1. Employee Internet abuse – more about this is mentioned in Chapter 9;
2. data leak/data breach – unauthorized disclosure of corporate information and data (accidental and intentional);
3. industrial espionage (corporate "spying" activities);
4. damage assessment (following an incident);
5. criminal fraud and deception cases;
6. criminal cases (many criminals simply store information on computers, intentionally or unwittingly) and countless others;
7. copyright violation – more about this is mentioned in Chapter 10 (in CD).

Figure 7.1 shows the kind of data you "see" using forensics tools.

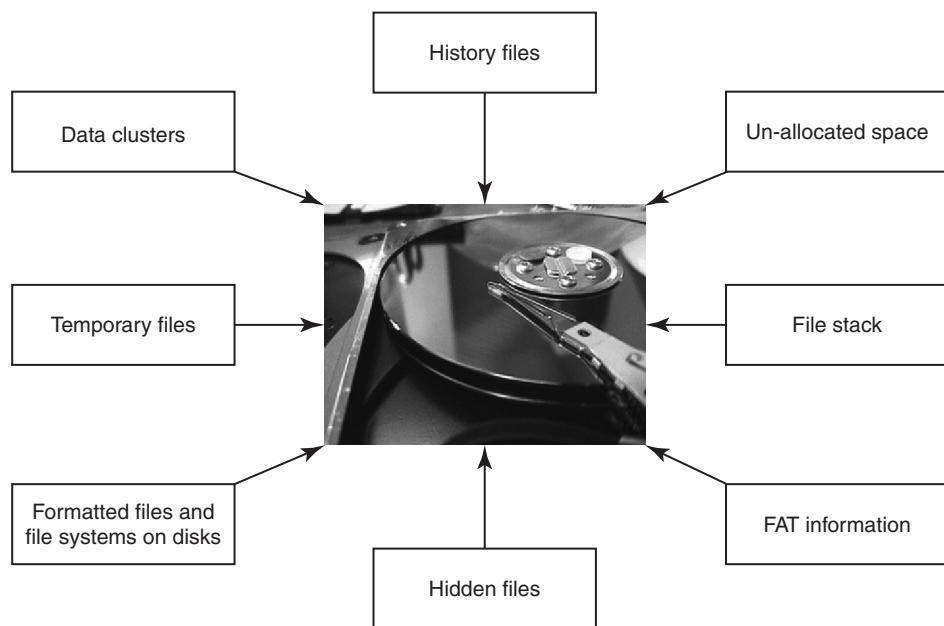


Figure 7.1 | Data seen using forensics tools. FAT means file allocation table.

Using digital forensics techniques, one can:

1. Corroborate and clarify evidence otherwise discovered.
2. Generate investigative leads for follow-up and verification in other ways.
3. Provide help to verify an intrusion hypothesis.
4. Eliminate incorrect assumptions.

Box 7.2 Differences between Forensics Policy and Security Policy

Often people get confused between "forensics policy" and "security policy." They think that the meaning of two terms is the same; however, this is not true. *Security policy* is a statement that clearly specifies the allowed and disallowed elements with regard to security. It partitions the system states into "secure" and "unauthorized" security policy that helps implement mechanisms to enforce system security policy. On the other hand, *forensics policy* is a statement that clearly states which assets are forensically important. It also specifies data needed for investigation into breach of those assets.

Forensics policy partitions space of all possible breaches or criminal activity into sets of events that are forensically noteworthy and those that are not. It allows for mechanisms or design decisions to enforce the policy. Here is another way to understand the difference between *security policy* and *forensics policy* – violation of security policy leads to insecure information systems/application with vulnerabilities arising due to consequences of break-in or insider misuse. On the other hand, violation of forensics policy means lack of evidence which results in the loss of ability of an organization to prove guilty the people who are involved in cybercrime incidence.

The "goals" defined by forensics policies are different than those defined by security policies. Goals of forensics policies deal with assets, data and possible storage issues. They capture digital evidence; therefore, forensics integrity of data is preserved. They capture enough data to ensure

Box 7.2 Differences between . . . (Continued)

that prosecution is possible. Forensics policy goals specify events that must be handled and data that must be preserved. Events not included in the policy will not need associated data. Here is an example of forensics policy:

1. Goal is to capture data from network intrusions for possible prosecution.
2. This (forensics) policy states that all events identified as intrusions will have their associated data captured and preserved.
3. Enforcement mechanisms: routine preservation of IDS, firewall, router and web server logs for some configurable length of time.

Here is another example of organizational level operating rules derived from an organization's forensics policy:

1. All access to Oracle DB must be monitored.
2. Access logs and administration logs to Oracle DB will be preserved for no less than 1 year.
3. Access and activity to web server is monitored.
4. Apache web server logs will be preserved for 1 year/6 months.
5. Firewall and Snort logs will be preserved for 1 year.
6. Router logs will be preserved for 6 months.
7. Network will be tested every 6 months for congestion situation by overloading it until it begins to drop traffic.
8. Network capacity will be increased before traffic hits the level where packets will be dropped.

7.4 The Need for Computer Forensics

The convergence of Information and Communications Technology (ICT) advances and the pervasive use of computers worldwide together have brought about many advantages to mankind. At the same time, this tremendously high technical capacity of modern computers/computing devices provides avenues for misuse as well as opportunities for committing crime. This has lead to new risks for computer users and also increased opportunities for social harm. The users, businesses and organizations worldwide have to live with a constant threat from hackers who use a variety of techniques and tools to break into computer systems, steal information, change data and cause havoc. The topic of “threats to information systems” is thoroughly discussed in Ref. #12, Books, Further Reading. The widespread use of computer forensics is the result of two factors: the increasing dependence of law enforcement on digital evidence and the ubiquity of computers that followed from the microcomputer revolution.

Box 7.3 Digital Forensics Investigations and E-Discovery

Digital evidence plays a crucial role in the threat management life cycle, from incident response to high-stakes corporate litigation. Forensics discoveries provide the ability to search and analyze various pieces of potential evidence of electronic nature. Evidence can involve computer hard drives, portable storage, floppy diskettes, portable music players and PDAs, just to name a few.

All forms of evidence are verified and duplicated prior to investigation to ensure the *integrity* of the evidence for litigation purposes if needed. Managers who are responsible for litigation tend to take help from forensics professionals to solve a growing range of evidentiary and investigative challenges.

Key evidence often resides on more than a user hard drive or file server, requiring the capture and analysis of evidence from enterprise productivity servers, network logs or proprietary databases.

Box 7.3 Digital Forensics . . . (Continued)

Many threats arise from illegal Internet activities that extend beyond the firewall and require new investigative and forensics approaches. Users are becoming more sophisticated and so are their efforts to circumvent security policies or encrypt, delete or destroy digital evidence. Forensics professionals need supporting solution for the acquisition, management and analysis of digital evidence. Such computer forensics services include the following:

1. Data culling and targeting;
2. discovery/subpoena process;
3. production of evidence;
4. expert affidavit support;
5. criminal/civil testimony;
6. cell phone forensics;
7. PDA forensics.

Specific client requests for forensics evidence extracting solution support include:

1. Index of files on hard drive;
2. index of recovered files;
3. MS Office/user generated document extraction;
4. unique E-Mail address extraction;
5. Internet activity/history;
6. storage of forensics image for 1 year (additional charges then apply);
7. keywords search;
8. chain of custody (see Section 7.8, Figs. 7.10 and 7.11, Boxes 7.4 and 7.12);
9. mail indexing;
10. deleted file/folder recovery;
11. office document recovery;
12. metadata indexing;
13. conversion to PDF;
14. log extraction;
15. instant messaging history recovery;
16. password recovery;
17. format for forensics extracts (DVD, CD, HDD, other);
18. network acquisitions.

Such types of computer evidences are important because quite often the evidence becomes the deciding factor in a criminal, civil or employee dismissal action. Investigations involving *trade secrets*, commercial disputes, and misdemeanor and felony crimes can be won or lost solely with the introduction of recovered E-Mail and other electronic documentation. If someone makes an attempt to delete, erase or otherwise hide critical evidence, you need the competent data recovery capabilities of forensics discoveries. Evidence that may not be known to attorneys may exist and often can be found during the forensics process. Also, timelines of computer usage is of help in crafting deposition questions and in targeting witnesses for interview.

Computer users typically "delete" incriminating and/or sensitive computer files (e.g., using tools such as "Deep Freeze," a software tool that is actually meant to protect your computer) but the information may still exist in slack space on the computer's hard drive that is hidden (do see the list of links provided at the end of this box). This computer data may linger for months or even years. However, it can be recovered and documented using computer forensics methods and techniques. Unfortunately, there are many examples of computer usage in violation of company policy. Sexual harassment, embezzlement, theft of trade secrets, abuse of the Internet and unauthorized outside employment on company time are just a few examples of violation that warrant a forensics examination of a computer. Even in investigations where hard drives are reformatted in an attempt to hide evidence, forensics discoveries can still potentially recover critical information (do see the list of links provided at the end of this box). Forensic discoveries can also aid in recovering passwords for critical files that have been maliciously set or changed.

Box 7.3 Digital Forensics . . . (Continued)

There are further challenges; for example, many times, computers are reissued when employees leave. Computer that is used continuously may destroy the incriminating evidence that can be used against a former disgruntled employee. Also, constant use of the computer may raise questions as to who created the incriminating evidence and when. To prevent these problems and to preserve potentially valuable information, it is recommended that a strict chain of custody should be followed and the subject computer should be shutdown, that is, the computer on which digital evidence is believed to be residing.

Useful links – The following link has the video where a digital forensics expert explains about E-Discovery and other aspects showing usefulness of digital forensics:
http://www.youtube.com/watch?v=y_BLtefQv40 (27 February 2010).

The following links (accessed on 28 March 2010) provide information about various tools including Deep Freeze:

1. <http://software.informer.com/getfree-deep-format-recover/> (Deep Format Recover Tools);
2. http://www.astahost.com/info.php/Deep-Freeze-Partition_t2571.html (Deep Freeze-related Blog);
3. <http://www.hochstadt.com/protecting-your-computer-using-deep-freeze> (an article here explains how you can protect your computer using “Deep Freeze”);
4. <http://technodata.blogspot.com/2006/11/how-to-format-hard-disk-by-disk.html> (this article explains how to format the hard disk);
5. <http://www.softlist.net/search/deep-freeze-2000-xp/> (Deep Freeze 200 XP Free Downloads);
6. <http://www.pctechguide.com/forums/ubbthreads.php/topics/4391/Hard%20Disk%20re-format> (technical blog);
7. <http://www.bluescreengone.com/comparison.htm> (Table showing Comparison of various Data Recovery and Data Formatting Tools);
8. <http://www.soft82.com/free/remote-yahoo-password-stealer/> (Yahoo Password Recovery Tools and many similar utilities);
9. <http://www.soft82.com/free/free-youtube-downloader-mp3/> (link to many free downloads of useful utilities).

The media, on which clues related to cybercrime reside, would vary from case to case. There are many challenges for the forensics investigator because storage devices are getting miniaturized due to advances in electronic technology; for example, external storage devices such as mini hard disks (pen drives) are available in amazing shapes (Fig. 7.2).

Looking for digital forensics evidence (DFE) is like looking for a needle in the haystack. Here is a way to illustrate why there is always the need for forensics software on suspect media – the capacity of a typical regular hard disk is 500 GB (gigabytes). In an A4 size page, there are approximately 4,160 bytes (52 lines × 80 Characters = 4,160 bytes assuming 1 byte per character). This is equivalent to 4 KB (kilobytes). An A4 size of paper sheet has thickness of 0.004 inches. Data of 4 MB (megabyte; 1,000 times of 4 KB) when printed on A4 size of paper would be 4 inches thick. Data of 4 GB if printed on A4 sheet would be 4,000 inches, that is, 1,000 times of 4 MB. This would turn out to be 4 inches thick. The printout of 500 GB would be 500,000 inches! It would be virtually impossible to “retrieve” relevant forensics data from this heap!! There comes the help from forensics software – it helps sieve relevant data from the irrelevant mass (vital few from trivial many as the proverb goes).

The term “chain of custody” is important (see Box 7.4).



Chain of custody means the chronological documentation trail, etc. that indicates the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic.



Figure 7.2 | Hidden and miniaturized storage media.

Sources: <http://www.ghdigital.com>; <http://www.technology-guide.co.uk>; <http://designyoutrust.com>; <http://gadgethobby.com>

Box 7.4 Chain of Custody Example

The basic idea behind ensuring "chain of custody" is to ensure that the "evidence" is NOT tampered with. The recovery of a "crime weapon" at the murder scene would be an example of "chain of custody." This is explained below.

Case Study

Officer Amar collects the knife and places it into a container, then gives it to forensics technician Balan. Forensics technician Balan takes the knife to the laboratory and collects fingerprints and other evidence from the knife. He then gives the knife and all evidence gathered from the knife to evidence clerk Charu. Charu then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife and original copies of the lifted fingerprints).

The chain of custody requires that from the moment the evidence is collected, every transfer of evidence from one person to another person should be documented as it helps to prove that nobody else could have accessed that evidence. It is advisable to keep the number of evidence transfers as low as possible. In the courtroom, if the defendant challenges the chain of custody of the evidence, it can be proven that the knife in the evidence room is the same knife as found at the crime scene. However, if due to some discrepancies it cannot be proven who had the knife at a particular point in time, then the chain of custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.

In a broader perspective “evidence” includes everything that is used to determine or demonstrate the truth of an assertion. Evidence can be used in court to convict people who are believed to have committed crimes; therefore, evidence must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct that can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The purpose behind recording the chain of custody is to establish that the alleged evidence is, indeed, related to the alleged crime, that is, the purpose is to establish the integrity of the evidence. In the context of conventional crimes, establishing “chain of custody” is especially important when the evidence consists of fungible goods.



“Fungibility” means the extent to which the components of an operation or product can be interchanged with similar components without decreasing the value of the operation or product.

For a person to be considered as “identifiable person,” he/she must always have the physical custody of a piece of evidence. Practically speaking, this means that a police officer or detective will take charge of a piece of evidence, document its collection and hand it over to an evidence clerk for storage in a secure place. All such transactions as well as every succeeding transaction between evidence collection and its appearance in court need to be completely documented chronologically to withstand legal challenges to the authenticity of the evidence. Documentation must include conditions under which the evidence is collected, the identity of all those who handled the evidence, duration of evidence custody, security conditions while handling or storing the evidence and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).



Chain of custody is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.

Chain of custody is particularly important in situations where sampling can identify the existence of contamination and can be used to identify the responsible party. In Section 7.8, the relevance of chain of custody is explained in the context of computer/digital forensics.

7.5 Cyberforensics and Digital Evidence

Cyberforensics can be divided into two domains:

1. Computer forensics;
2. network forensics.

Many security threats are possible through computer networks (to know more on this, readers can refer to Ref. 11, Books, Further Reading). Therefore, “network forensics”^[26] assumes importance in the context of cybercrime.



Network forensics is the study of network traffic to search for truth in civil, criminal and administrative matters to protect users and resources from exploitation, invasion of privacy and any other crime fostered by the continual expansion of network connectivity.

As compared to the “physical” evidence, “digital evidence” is different in nature because it has some unique characteristics. First of all, digital evidence is much easier to change/manipulate! Second, “perfect” digital copies can be made without harming original. At the same time the integrity of digital evidence can be proven. Another subtle aspect (of digital evidence) is that it is usually in the form of the “image” – this means that it is convenient and possible to create a defensible “clone” of storage device. Different information (clues) can be found at different levels of abstraction. Understanding the uniqueness of digital evidence is important for appreciating the phases involved in a digital forensics investigation and maintaining the “chain of custody” (refer to Section 7.8, Figs. 7.10 and 7.11, Boxes 7.4 and 7.12).

There are many forms of cybercrimes: sexual harassment cases – memos, letters, E-Mails; obscene chats or embezzlement cases – spreadsheets, memos, letters, E-Mails, online banking information; corporate espionage by way of memos, letters, E-Mails and chats; and frauds through memos, letters, spreadsheets and E-Mails. In case of computer crimes/cybercrimes, computer forensics helps. Computer forensics experts know the techniques to retrieve the data from files listed in standard directory search, hidden files, deleted files, deleted E-Mail and passwords, login IDs, encrypted files, hidden partitions, etc. Typically, the evidences reside on computer systems, user created files, user protected files, computer created files and on computer networks. Computer systems have the following:

1. Logical file system that consists of
 - File system: It includes files, volumes, directories and folders, *file allocation tables* (FAT) as in the older version of Windows Operating System, clusters, partitions, sectors.
 - Random access memory.
 - Physical storage media: It has magnetic force microscopy that can be used to recover data from overwritten area.
 - (a) Slack space: It is a space allocated to the file but is not actually used due to internal fragmentation and
 - (b) unallocated space.
2. User created files: It consists of address books, audio/video files, calendars, database files, spreadsheets, E-Mails, Internet bookmarks, documents and text files.
3. Computer created files: It consists of backups, cookies, configuration files, history files, log files, swap files, system files, temporary files, etc.
4. Computer networks: It consists of the Application Layer, the Transportation Layer, the Network Layer, the Datalink Layer.

Readers who are not savvy with these terms and concepts can refer to Ref. #11, Books, Further Reading. The Open System Interconnection (OSI) Layer Model (Application Layers, Transportation Layer, Datalink Layer, etc.) is also explained in Ref. #11, Books, Further Reading.

Box 7.5 The Father of Forensics Science – the Sherlock Holmes of France

The year 1877–1966 was the era of Dr. Edmond Locard. He is considered as the pioneer in forensics science and was popularly known as the Sherlock Holmes of France. He formulated the basic principle of forensics science: “Every contact leaves a trace.” This came to be known as Locard’s exchange principle. Following is one of his most famous quotes:

Wherever he steps, wherever he touches, whatever he leaves, even without consciousness, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or

Box 7.5 \ The Father of . . . (Continued)

semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. In other words, Whenever two human beings come into contact, something from one is exchanged to the other, that is, dust, skin cells, hair, etc."

For a short video clip that demonstrates how "Locard Principle" works, one can visit the link:
<http://science.howstuffworks.com/locards-exchange-principle.htm/printable> (11 September 2009).

Locard studied medicine and law at Lyon, eventually becoming the assistant of Alexandre Lacassagne, a criminologist and professor. He held this post until 1910, when he began the foundation of his criminal laboratory. He produced a monumental seven-volume work, *Traité de Criminalistique*, and in 1918, developed 12 matching points for fingerprint identification. He continued with his research until his death in 1966.

7.5.1 The Rules of Evidence

This is a very important discussion, especially, for those who are students of legal courses. It was mentioned in Chapter 6 (Section 6.4) that the Indian IT Act amended the Indian Evidence Act. According to the "Indian Evidence Act 1872," "Evidence" means and includes:

1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called *oral evidence*.
2. All documents that are produced for the inspection of the court are called *documentary evidence*.

Legal community believes that "electronic evidence" is a new breed of evidence. They also, at times, have an apprehension that the law of evidence as per Indian Evidence Act of 1872 may not hold good for electronic evidence. Some lawyers express doubts and apprehensions about the process of leading electronic evidence in the courts. However, this is not true; the traditional principles of leading evidence, along with certain newly added provisions in the Indian Evidence Act 1972 through the Information Technology Act (ITA) 2000, constitute the body of law applicable to electronic evidence. The challenges, however, need to be understood from the "rules of evidence" perspective.



Paper evidence, the process is clear and intuitively obvious. Digital evidence by its very nature is invisible to the eye. Therefore, the evidence must be developed using tools other than the human eye.

It is only logical that the process used in the case of digital evidence mimic the process that is used for paper evidence. As each step requires the use of tools or knowledge, the process must be documented, reliable and repeatable. The process itself must be understandable to the members of the court. Acquisition of digital evidence is both a legal and technical problem. In fact, these two aspects are irrevocably related. The law specifies what can be seized, under what conditions, from whom and from where. It requires to determine what particular piece of digital evidence is required for examination, that is, is it a particular file or a word processing document or an executable program, etc. It may also require examination to determine where a particular piece of evidence is physically located. Is the file on a local hard drive or is it on a server

located in another legal jurisdiction? In short, it may be necessary to show a technical basis for obtaining the legal authority to search. Likewise, it may require technical skills to actually accomplish the search. The product of this phase is usually raw media, devoid of meaning or usefulness.

There are number of contexts involved in actually identifying a piece of digital evidence:

1. **Physical context:** It must be definable in its physical form, that is, it should reside on a specific piece of media.
2. **Logical context:** It must be identifiable as to its logical position, that is, where does it reside relative to the file system.
3. **Legal context:** We must place the evidence in the correct context to read its meaning. This may require looking at the evidence as machine language, for example, American Standard Code for Information Interchange (ASCII).

The path taken by digital evidence can be conceptually depicted as shown in Fig. 7.3.

Digital evidence originates from a number of sources such as seized computer hard drives and backup media, real-time E-Mail messages, chat room logs, Internet service provider records, webpages, digital network traffic, local and virtual databases, digital directories, wireless devices, memory cards, digital cameras, etc. Digital forensics examiners must consider the trustworthiness of this digital data. Many vendors provide technology solutions to extract this digital data from these devices and networks. Once the extraction of the digital evidence has been accomplished, protecting the digital integrity becomes paramount concern for investigators, prosecutors and those accused.

Similarly for the evidence in regular crimes, it is important to “isolate” the potential evidence. Some important tips are – do not turn ON the computer or review media, restrict physical and remote access, unplug computer power, network and phone line, and document times, people and steps taken. A point to note is that the need to unplug the computer power depends on the crime situation and the type of analysis required. For example, for live analysis of the digital evidence, it would not be advisable to unplug the power. Therefore, it is best to involve qualified specialists early in the process. Following are some guidelines for the (digital) evidence collection phase:

1. Adhere to your site’s security policy and engage the appropriate incident handling and law enforcement personnel.
2. Capture a picture of the system as accurately as possible.

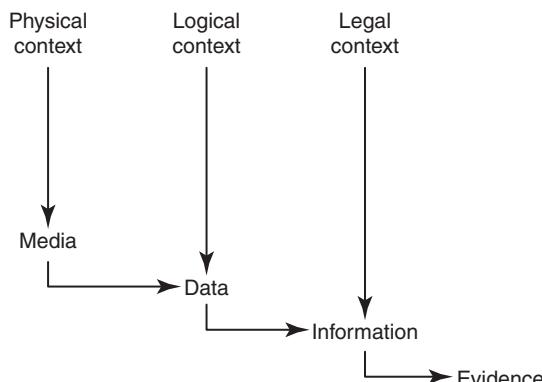


Figure 7.3 | Path of the digital evidence.

3. Keep detailed notes with dates and times. If possible, generate an automatic transcript (e.g., on Unix systems the “script” program can be used; however, the output file it generates should not be given to media as that is a part of the evidence). Notes and printouts should be signed and dated.
4. Note the difference between the system clock and Coordinated Universal Time (UTC). For each timestamp provided, indicate whether UTC or local time is used (since 1972 over 40 countries throughout the world have adopted UTC as their official time source).
5. Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.
6. Minimize changes to the data as you are collecting it. This is not limited to content changes; avoid updating file or directory access times.
7. Remove external avenues for change.
8. When confronted with a choice between collection and analysis you should do collection first and analysis later.
9. Needless to say, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility, particularly, in a crisis. If possible, procedures should be automated for reasons of speed and accuracy. Being methodical always helps.
10. For each device, a systematic approach should be adopted to follow the guidelines laid down in your collection procedure. Speed will often be critical; therefore, where there are a number of devices requiring examination, it may be appropriate to spread the work among your team to collect the evidence in parallel. However, on a single given system collection should be done step by step.
11. Proceed from the volatile to the less volatile; order of volatility is as follows:
 - Registers, cache (most volatile, i.e., contents lost as soon as the power is turned OFF);
 - routing table, Address Resolution Protocol (ARP) cache, process table, kernel statistics, memory;
 - temporary file systems;
 - disk;
 - remote logging and monitoring data that is relevant to the system in question;
 - physical configuration and network topology;
 - archival media (least volatile, i.e., holds data even after power is turned OFF).
12. You should make a bit-level copy of the system’s media. If you wish to do forensics analysis you should make a bit-level copy of your evidence copy for that purpose, as your analysis will almost certainly alter file access times. *Try to avoid doing forensics on the evidence copy.*



Address Resolution Protocol (ARP) is a very important part of IP networking. ARP is used to connect OSI Layer 3 (Network) to OSI Layer 2 (Datalink). For most of us this means that ARP is used to link our IP addressing to our Ethernet addressing (MAC Addressing). For you to communicate with any device on your network, you must have the Ethernet MAC address for that device. If the device is not on your LAN, you go through your default gateway (your router). In this case, your router will be the destination MAC address that your PC will communicate with. There are two types of ARP entries: static and dynamic. Most of the time, you will use dynamic ARP entries. What this means is that the ARP entry (the Ethernet MAC to IP address link) is kept on a device for some period of time, as long as it is being used. The opposite of a dynamic ARP entry is static ARP entry. With a static ARP entry, you are manually entering the link between the Ethernet MAC address and the IP address. Because of management headaches and the lack of significant negatives to using dynamic ARP entries, dynamic ARP entries are used most of the time.

7.6 Forensics Analysis of E-Mail

In Chapter 2 (Section 2.3.1), it was mentioned how criminals can use fake mails for various cybercrime offenses. There are tools available that help create fake mails. *Forensics analysis of E-Mails* is an important aspect of cyberforensics analysis – it helps establish the authenticity of an E-Mail when suspected. This aspect is explained in this section – we start with understanding E-Mail components and then the E-Mail header structure is explained. E-Mails are now the most common means of communication worldwide and are often the subject of forensics analysis if this happens to constitute “digital evidence.” Owing to the rising pressures from regulatory agencies and also due to possible litigations in global businesses, organizations are obligated to electronically store information to support discovery and disclosure requests. In this section, we want to discuss how E-Mail messages/IDs can help in forensic analysis of cybercrimes.

An E-Mail system is the hardware and software that controls the flow of E-Mail. The two most important components of an E-Mail system are the E-Mail server and the E-Mail gateway. *E-Mail servers* are computers that forward, collect, store and deliver E-Mail to their clients and E-Mail gateways are the connections between E-Mail servers. *Mail server software* is a network server software that controls the flow of E-Mail and the mail client software helps each user read, compose, send and delete messages. An E-Mail consists of two parts, the header and the body. *Message headers* are the important part for investigating E-Mail messages and hence it will be discussed in detail in this section. The “header” of an E-Mail is very important from forensics point of view – a full header view of an E-Mail provides the entire path of E-Mail’s journey from its origin to its destination. The header view includes the originating Internet Protocol (IP) address and other useful information (see Table 7.1). There is usually a link provided on the E-Mail from its origin to its destination.

Box 7.6 Electronic Messages and the Indian Evidence Act

Section 88 of the Indian Evidence Act is about *Presumption as to telegraphic messages*. It states the following:

Presumption as to telegraphic messages. The Court may presume that a message, forwarded from a telegraph office to the person to whom such message purports to be addressed, corresponds with a message delivered for transmission at the office from which the message purports to be sent; but the Court shall not make any presumption as to the person by whom such message was delivered for transmission.

As per Section 66A(C) of Indian IT Act any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to 2 or 3 years and with fine – refer to URL http://cybercrime.planetindia.net/ch11_2008.htm

In terms of the amended Indian ITA 2000, that is, the ITA 2008 (notified on 5 February 2008), it is interesting to know how the court thinks when it comes to evidences based on E-Mails. As mentioned at the beginning, according to the Section 88A of the Indian Evidence Act, the court may presume that an electronic message forwarded by an originator through an E-Mail server to the addresses, to whom the message purports to be addressed, corresponds with the message as fed into the person’s computer for transmission. However, the court shall not make any “presumption” as to the person by whom such message was sent. Furthermore, it is interesting to note the word “may presume” and the expressions “shall presume” and “conclusive proof.”

1. The word “may presume” denotes that the court may either regard such fact as proved until it is disapproved, or may call for proof of it (Section 4 of the Indian Evidence Act 1872).
2. The word “shall presume” denotes that whenever it is directed by this Act that the court shall presume a fact, it shall regard such fact as proved, unless and until it is disapproved.

Box 7.6 Electronic Messages . . . (Continued)

3. The word "conclusive proof" denotes that when one fact is declared by this Act to be conclusive proof of another, the court shall, on proof of the one fact, regard the other as proved, and shall not allow evidence to be given for the purpose of disapproving it.

Source: Refer to Section 4 of the Indian Evidence Act. It can be downloaded from <http://chddistrictcourts.gov.in/THE%20INDIAN%20EVIDENCE%20ACT.pdf> (22 November 2008).

Table 7.1 | E-Mail header example

1. Return-Path: <secret@hotmail.com>
2. Received: from mailhub-1.net.treas.gov ([10.7.14.10]) by nccmail.usss.treas.gov for <avenit@usss.treas.gov>; Fri, 18 Feb 2000 11:46:07-0500
3. Received: from mx-relay.treas.gov ([199.196.144.6]) by tias4.net.treas.gov via smptd (for mailhub.net.treas.gov [10.7.8.10]) with SMTP; 18 Feb 2000 16:55:44
4. Received: from hotmail.com (f7.law4.hotmail.com [216.33.149.7]) by mx-relay2.treas.gov for <avenit@usss.treas.gov>; Fri, 18 Feb 2000 11:55:44 -0500 (EST)
5. Message-ID: <20000218165543.56965.qmail@hotmail.com>
6. Received: from 199.196.144.42 by www.hotmail.com with HTTP; Fri, 18 Feb 2000 08:55:43
7. X-Originating-IP: [199.196.144.42]
8. From: "Secret" <secret@hotmail.com>
9. To: avenit@usss.treas.gov
10. CC: smith@aol.com

Header information varies with E-Mail service provider, E-Mail applications and system configuration. As we know, the header part carries information that is needed for E-Mail routing, subject line and time stamps whereas the body contains the actual message/data of an E-Mail. The header and the body are separated by a blank line. The header contains several mandatory and optional fields, trace information and heading fields. The E-Mail header is a sequence of fields (it may not be in a particular order), each consisting of a field name and a field value. An example of a heading field would be: To: xyz@abccom.in. Headers on E-Mail can easily be "spoofed" by spammers and other irresponsible network users. E-Mails, when used in cyberforensics investigation, must get uniquely identified, if, for example, an E-Mail is suspected to be one of the evidence sources.

As mentioned earlier, the body of an E-Mail is separated from the header and it might also contain attachments in the form of MIME or SMIME (also known as S/MIME – secure/multipurpose Internet mail extensions). It is a protocol that provides digital signatures and encryption of Internet MIME messages. It is an encoding protocol (readers can visit the link at <http://email.about.com/cs/standards/a/mime.htm> to understand how MIME works for E-Mails).

We have mentioned previously that an E-Mail has two parts and header is one of those two parts. However, there is a header protocol: when an E-Mail message is sent, the user typically controls only the recipient line(s), that is, *To*, *Cc* and *Bcc*, if mentioned, and the *Subject* and *Date*. The rest of the header information is added by mail software while it is processed. Along the E-Mails route, a server can add or delete lines (anonymous remailer). Table 7.1 shows example of a mail header; for ease of understanding, each element of the header has been numbered. The discussion that follows is with reference to those numbers. *Header Protocol Analysis* is important for investigating evidence that may come in form of an E-Mail.

In Table 7.1, elements 2, 3 and 4 show the route taken by the message from sending to delivery. Every computer that receives this message adds a "*Received:* field" with its complete address and time stamp; this

helps in tracking delivery problems. Element 5 of the mail header is the Message-ID, a unique identifier for this specific message. The Message-ID is logged and it can be traced through computers that are on the message route if there is a need to track the mail. Element 6 of the E-Mail header shows where the E-Mail was first received from with the IP address of the sender. It also shows the date and time when the message was sent. In this regard, it is important to understand the difference between simple mail transfer protocol (SMTP) and Hypertext Transfer Protocol (HTTP). HTTP is used to transfer displayable webpages and related files whereas SMTP is used to transfer E-Mail. Thus, SMTP is a protocol for sending E-Mail messages between servers whereas HTTP is a set of rules used to browse through Internet commonly used with web browsers such as Internet Explorer, Firefox). When you request, E-Mail logs you and you should ensure that you get them from the right server.

Next, consider element 7 of the sample mail header shown in Table 7.1 – it shows the originating IP address of the sender, but without the date and time the IP address will not allow you to identify the specific user. This may or may not be present in headers. If the IP address is a “Static” Address, you *will* be able to identify the specific user (most IP addresses are “dynamically” assigned). Element 8 indicates the name and E-Mail address of the message originator, that is, the “sender.” Generally, this is the domain name we want to trace. Element 9 shows the name and E-Mail address of the primary recipient; the address may be for a mailing list (sales_dep@company.com) or systemwide *alias* (avenit@usss.treas.gov) or a personal username. The next element, element 10, of the sample mail header lists the names and E-Mail addresses of the “courtesy copy” recipients of the message. Some E-Mails may have “Bcc:” recipients as well; these “blind carbon copy” recipients get copies of the message, however their names and addresses are not visible in the headers.

Once we get the IP address our task is to find the Internet service provider details. The following links are worth visiting:

1. www.all-nettools.com (among other tools; a link to E-Mail tools is available here);
2. www.ip2location.com (there is a utility here that helps you know where your Internet visitors are coming from, that is, which country, which state, which city, which Internet service provider, which domain name, which connection type, which ZIP code, etc. It helps you trace an IP address to Country, Region, City, Latitude, Longitude, ZIP Code, Time Zone, Connection Speed, Internet service provider, Domain Name, IDD Country Code, Area Code, Weather Station Code and Name).
3. www.domaintools.com (there are DNS tool and many other tools available here);
4. www.dnsstuff.com (domain/E-Mail-related tools are accessible from this site);
5. http://www.hackingspirits.com/cyb_forensics/fsic_articles/trace_emails.html is a good link to know tracing the origin of an E-Mail, that is, locating countries from an IP address.

The Internet service provider plays an important role in E-Mail forensics. The Internet service provider provides Internet access to businesses, organizations, schools, colleges and individuals. Examples of Internet service provider are VSNL (Videsh Sanchar Nigam Limited), Sify, Hathway, Rolta, MTNL/BSNL, Reliance, etc. The details available from the Internet service provider are name, address and contact number of the subscriber of the Internet facility, type of IP address, any other relevant information with regard to IP address at a particular given date and time, usage details, etc.

Box 7.7 Points to Remember when you Use E-Mail as an Evidence

1. Ensure the use of E-Mail is subject to agreed procedures, which are supported and enforced by management at a high level. Acceptable Use Policies ought to prescribe good usage and identify bad usage.

Box 7.7 Points to Remember . . . (Continued)

2. Train users of E-Mail about acceptable use of E-Mail, and about their rights and the obligations expected of them.
3. Implement access control mechanisms to computer systems – so that its use can be attributed to a person, a terminal, a date and a time.
4. Ensure computer systems are kept safe and secure so that the systems and the data within are protected from unauthorized access and accidental or deliberate loss and damage.
5. Retention and deletion of E-Mail should be organization-defined and not user-defined. Individual users should not have any discretion as to the categories of E-Mails that should be retained or deleted.
6. Implement a solution that archives and stores E-Mails centrally. The archive should support all the main file formats and also retain metadata.
7. The archive should classify E-Mails entering the archive at the point of entry. The archive should prevent the entry of duplicates.
8. Make sure that the archiving platform facilitates the exporting of evidence as files as a part of the E-Discovery process.
9. Implement an archiving solution that allows full search and retrieval. Metadata should be searchable as should content.
10. Enable logging of all events acting on the archive. The logs should be retained as part of the archive, for auditing and verification purposes.
11. Provide contingency for continuity of both archiving and discovery in the event of an outage.
12. Ensure the archiving platform supports the marking-up of files so that privileged materials can be withheld and/or redacted during E-Discovery.

E-Mail headers are organized bottom-up. This means that the E-Mail was handed from the machines at the bottom of the E-Mail header to the ones at the top of it. These machines are referred to as Message Transfer Agents (MTAs) and each of them adds a “received” section to the E-Mail header, sometimes referred to as “received header.” This is similar to postmarks used in conventional postal systems. The order of the “received” sections is like a stack of pancakes, with the one receiving the E-Mail last at the top of the stack. Refer to Fig. 7.4 – note that there were three received sections (elements 2, 3 and 4 in Table 7.1). This means that three MTAs were involved in the delivery of the E-Mail message with the one at the bottom being the one receiving the original message from the sender.

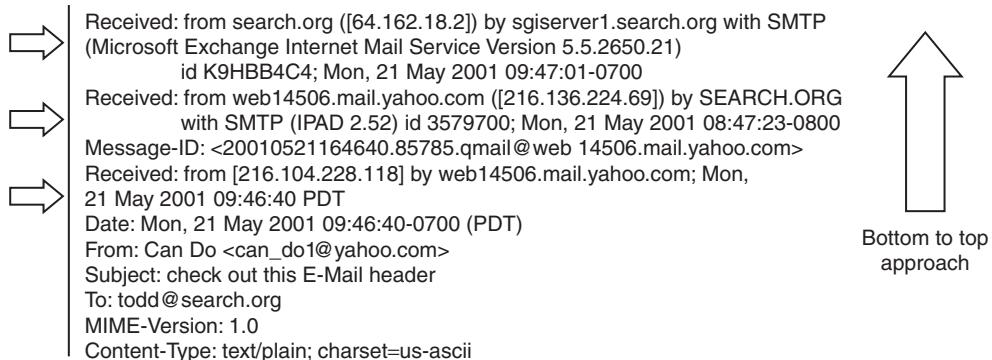


Figure 7.4 Bottom-up approach to tracing E-Mail source.

Source: “Tracing-eMail-Headers.pdf,” Marwan Al-Zarouni, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia. To see a visual example of tracing an E-Mail, readers can visit: <http://www.youtube.com/watch?v=hSvswzSy3oA&feature=related> (15 March 2010). It shows a video clip with demonstrating an E-Mail.



E-Mail tracing is done by examining the header information contained in E-Mail messages to determine their source.

While tracing E-Mails, the “header information” is included along with E-Mails either at the beginning or the end of E-Mail messages. A typical E-Mail header looks like as shown in Table 7.2.

To determine the source of the E-Mail, investigators must first examine the received section at the bottom of the header and work their way up in a bottom to top approach (see Fig. 7.4).

It is also important that during E-Mail investigation cases the logs of all servers in the received chain are examined as soon as possible. The time stamp is very important in E-Mail investigation cases because HTTP and SMTP logs get archived frequently, especially by large Internet service providers. When a log is archived, a considerable amount of time and effort is involved to retrieve and decompress the log files needed to trace E-Mails. Fake E-Mail creation tools are rampantly used by cybercriminals. Therefore, it is possible that some E-Mails have fake headers with fake “from” E-Mail addresses to fool investigators; however, extreme caution and careful scrutiny should be practiced in investigating every part of the E-Mail header (recall it in Chapter 2 in which it is explained that there are tools available that help create fake mails).

Typically, the sender’s E-Mail address can be found after the “From” section of the header. However, that is not the only place it can be found. It can also be found under other sections depending on the E-Mail client uses. These sections include the following (this is not the exhaustive list; it is just an example to give you some idea):

1. . X-originating E-Mail;
2. . X-sender;
3. . return-path.

At times, E-Mail addresses can suggest the method used to generate the E-Mail and the server that the E-Mail originated from (i.e., hotmail, outlook, corporate server, Internet service provider, etc.). However, E-Mail addresses should be viewed with caution by investigators as they can be easily faked. Note that some headers begin with an “X-,” this means that they are X-headers. You can use X-headers to sort and filter

Table 7.2 | Typical E-Mail header

-
1. Received: from search.org ([64.162.18.2]) by sgiserver1.search.org with SMTP (Microsoft Exchange Internet Mail Service
Version 5.5.2650.21)
id K9HBB4C4; Mon, 21 May 2001 09:47:01-0700
 2. Received: from web14506.mail.yahoo.com ([216.136.224.69]) by SEARCH.ORG
with SMTP (IPAD 2.52) id 3579700; Mon, 21 May 2001 08:47:23-0800
Message-ID: <20010521164640.85785.qmail@web14506.mail.yahoo.com>
 3. Received: from [216.104.228.118] by web14506.mail.yahoo.com; Mon, 21 May 2001 09:46:40 PDT
Date: Mon, 21 May 2001 09:46:40 -0700 (PDT)
From: Can Do <can_do1@yahoo.com>
Subject: check out this E-Mail header
To: todd@search.org
MIME-Version: 1.0
Content-Type: text/plain; charset = us-ascii
-

E-Mails sent by SourceForge. Depending on the context of the message, custom E-Mail headers (X-headers) are added to the E-Mail. The customer headers can be used by E-Mail agents and clients to filter and sort E-Mail. For example, both Outlook and Thunderbird support filtering on custom E-Mail headers. Thus, X-headers are inserted by E-Mail client programs or applications that use E-Mail to pass information to E-Mail handling programs for processing. They may be introduced by large vendors and picked up for use by others. In this way an X-header can be considered as a de facto standard. An example of this is the “X-Mailer” header which many E-Mail clients use to define the E-Mail client application and version used.

Next, let us understand how fake E-Mail addresses can be detected. The sender's E-Mail address can be easily faked and can be hard to detect. If the server mentioned in the bottom “received” section does not match the server of the E-Mail address, this suggests that the E-Mail address is a fake one. An example is shown in Table 7.3.

Note that in Table 7.3 the E-Mail address in the “From” field has “hotmail.com” as the domain for the E-Mail whereas in the received section of the header there is no hotmail server mentioned at all. This is clearly a forged (fake) E-Mail and it is very likely to have a fake “From” address. Also note that the time on the received section is Central European Standard Time (CEST), and hotmail.com servers are not in Europe.

Now let us consider Sendmail. Sendmail is a general purpose Internet work E-Mail routing facility that supports many kinds of mail-transfer and delivery methods, including SMTP used for E-Mail transport over the Internet. Sendmail is a descendant of the delivermail program that was written by Eric Allman. Sendmail is a well-known project of the free and open-source software (OSS) and Unix communities, and has spread both as free software and proprietary software. It is a very widely used MTA. MTAs send mail from one machine to another. Sendmail is not a client program, which you use to read your E-Mail but rather a behind-the-scenes program that actually moves your E-Mail over networks or the Internet to where you want it to go. If there is ever a situation to reconfigure Sendmail, you will also need to have the sendmail.cf package installed. In case you need documentation on Sendmail, you need to install the sendmail-doc package.

To uniquely identify each E-Mail, all MTAs use some sort of unique identifier. This identifier is referred to as “Message-ID.” *Message-ID field* is inserted into a header either by mail user agent (MUA) or the first MTA. Even though the Message-ID is optional as per RFC2822, it recommends using it. Sendmail, for example, is one MTA that handles E-Mail delivery and relaying process. Sendmail uses Message-ID for tracing E-Mails and for logging process IDs. It recommends including Message-ID in E-Mails and also recommends setting relevant macros in its configuration file to implement compulsory checking of Message-IDs.



A point to note is that unlike Spoofing other fields in the header, Spoofing Message-ID needs special knowledge. Sendmail-related FAQs are available at <http://www.sendmail.org/faq/section2>.

Deep analysis on Message-IDs may reveal some sort of information that will open a window to trace the source of an E-Mail. Also Message-ID will help to find a particular E-Mail log entry within a log file of E-Mail server.

Table 7.3 | Header of a fake mail (an example only)

Received: from infvic.it (adsl-98-201.38-151.net24.it [151.38.201.98])
by mail-relay2.bpvit.it (Postfix) with ESMTP id 2887550074
for <redazione@infvic.it>; Mon, 19 Apr 2004 10:41:54 +0200 (CEST)
From: sfiorillo@hotmail.com

Only technical envy spammers can spoof the Message-ID cleverly. So deep analysis on Message-IDs may reveal some sort of information that will open a window to trace the source of an E-Mail. Also the Message-ID will help to find a particular E-Mail log entry within a log file of E-Mail server. There are some commonalities between conventional mails and E-Mails; for example, like conventional mail service, when E-Mail is routed from source to destination all intermediate relay servers (SMTP) insert their stamp at the beginning of the header. This stamping procedure helps to trace the E-Mail if such a demand arises. The stamp consists of three fields, namely, "From," "SMTP-ID" and "For."

The text in Table 7.4 shows an E-Mail header that passed through several MTAs, that is, E-Mail header with several identifiers. Each MTA inserted a unique ID in the header of E-Mail. There are several identifiers in the header field of an E-Mail that may help to trace the source of the E-Mail but the context for Fig. 7.4 is limited to Sendmail Message-ID only. Analyzing intermediate SMTP-IDs is beyond the scope of this book. However, in this section, we have briefly discussed intermediate SMTP-IDs.

In the context of E-Mail, "messages" are viewed as having an "envelope" and "contents." The envelope contains information required to accomplish transmission and delivery. The contents contain the object to be delivered to the recipient. The delivery has to be at a valid E-Mail address and this is where the RFC2822 comes into picture.

7.6.1 RFC2822

RFC2822 is the Internet Message Format. According to the Internet specification RFC2822, there are several formats of valid E-Mail addresses, like joshi@host.net, john@[10.0.3.19], "Joshi Ganesh"@host.net or "Joshi Ganesh"@[10.0.3.19]. Many E-Mail address validators on the Web fail to recognize some of those valid E-Mail addresses. Some examples of invalid E-Mail addresses are as follows:

1. joshi@box@host.net: Two at signs (@) are not allowed;
2. joshi@host.net: Leading dot (.) is not allowed;
3. joshi@-host.net: Leading dash (-) is not allowed in on domain name;
4. joshi@host.web: Web is not a valid top level domain;
5. joshi@[10.0.3.1999]: Invalid IP address.

The RFC2822 standard applies only to the Internet Message Format and some of the semantics of message contents. It contains no specification of the information in the envelope. RFC2822 states that each E-Mail

Table 7.4 | E-Mail header with several identifiers

-
1. Received: from search.org ([64.162.18.2]) by sgiserver1.search.org with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2650.21)
id K9HBB4C4; Mon, 21 May 2001 09:47:01-0700
 2. Received: from web14506.mail.yahoo.com ([216.136.224.69]) by SEARCH.ORG with SMTP (IPAD 2.52) id 3579700; Mon, 21 May 2001 08:47:23-0800
Message-ID: <20010521164640.85785.qmail@web14506.mail.yahoo.com>
 3. Received: from [216.104.228.118] by web14506.mail.yahoo.com; Mon, 21 May 2001 09:46:40 PDT
Date: Mon, 21 May 2001 09:46:40-0700 (PDT)
From: <can_do1@yahoo.com>
Subject: check out this E-Mail header
To: todd@search.org
-

must have a “globally unique identifier.” This must be included into the header of an E-Mail. The RFC2822 also defines the syntax of Message-ID. It should be like a legitimate E-Mail address and it must be included within a pair of angle brackets. According to RFC2822, Message-ID can appear in three header fields: “Message-ID header,” “in-reply-to header” and “references header.” But Message-ID of the present E-Mail must be included against the “Message-ID” header. Remember that there are SPAM problems and to that, there is no simple solution. E-Mail headers cannot be trusted; not all E-Mail can be traced or authenticated. Only a legitimate mail typically can be traced. However, for SPAM and virus-generated E-Mail it is difficult to know if the headers are absolutely trustworthy.

Readers may refer to Ref. #2, Video Clips, Further Reading in which it is explained how to trace an E-Mail. To conclude this section, we say that tracing an E-Mail is an important forensics activity in instances where an E-Mail is believed to hold a queue for a cybercrime. Understanding the E-Mail header structure is important while tracing an E-Mail and we have discussed that so far. Readers, who are interested in learning about tracking E-Mails, can try out the tutorials available at the following links accessed on 6 December 2009:

1. <http://www.visualware.com/resources/tutorials/email.html> (both download and live demonstrations are available at this link);
2. <http://www.visualware.com/resources/tutorials/emailX.html> (a tutorial on E-Mail tracking tutorial is available here).

7.7 Digital Forensics Life Cycle

As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene. That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination. Figure 7.5 shows the process model for understanding a *seizure and handling of forensics evidence* legal framework. The cardinal rules to remember are that evidence:

1. is admissible;
2. is authentic;
3. is complete;
4. is reliable;
5. is understandable and believable.

Let us now understand what is involved in the digital forensics process.

7.7.1 The Digital Forensics Process

The digital forensics process needs to be understood in the legal context starting from preparation of the evidence to testifying. Digital forensics evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter to help jurors establish the facts of the case and support or refute legal theories of the case. The exhibits should be introduced and presented and/or challenged by properly qualified people using a properly applied methodology that addresses the legal theories at issue. The tie between technical issues associated with the digital forensics evidence and the legal theories is the job of “expert witnesses.”

As part of the court procedure, the exhibits are introduced as evidence by either side. *Testimony* is presented to establish the process to identify, collect, preserve, transport, store, analyze, interpret, attribute, and/or reconstruct the information contained in the exhibits and to establish, to the standard of proof required by the matter at hand, that the evidence reflects a sequence of events that is asserted to have produced it. The party must show not only the evidence to be admitted but must also establish that the evidence is

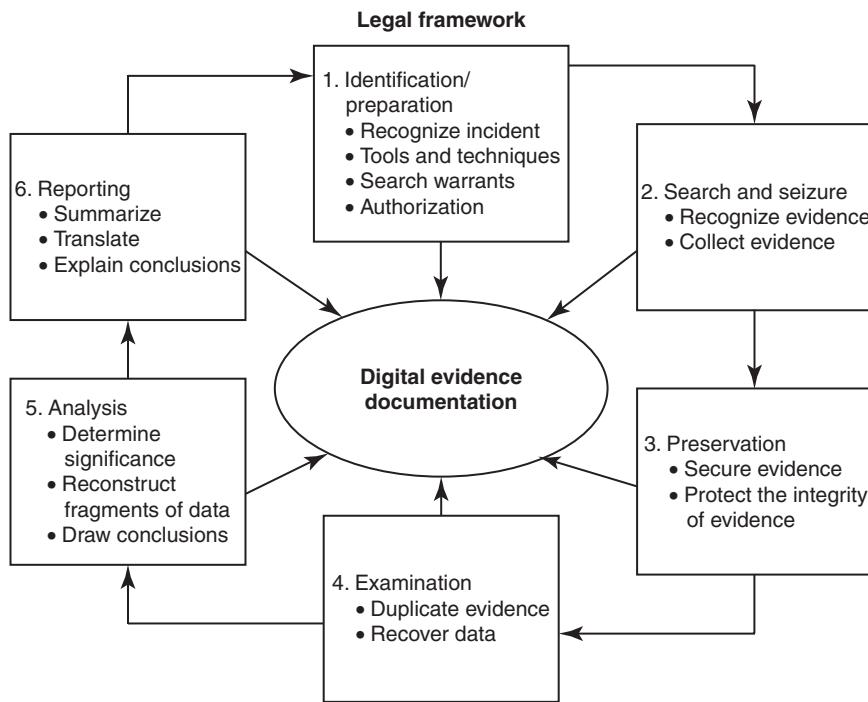


Figure 7.5 | Process model for understanding a seizure and handling of forensics evidence legal framework.

relevant, authentic and that the evidence presented is not the result of hearsay, original writing or the legal equivalent thereof, and more probative than prejudicial.

Usually the assumption is that adequate facts can be established for the introduction of an evidence exhibit. Under this assumption, people involved in the “chain of custody” need to testify a number of aspects relating to the evidence – the testimony would typically include the processes used for creating, handling and introducing the evidence, the method used for collecting the exhibit (i.e. the evidence artifacts) as well as the manner in which the exhibit is brought to court. These people also get involved to testify about the event sequences that may have produced the evidence exhibit. Digital forensics evidence is usually latent, that is, “hidden” in that it can only be seen by the trier of fact at the desired level of detail through the use of tools. In order for tools to be properly applied to a legal standard, it is required that the people who use these tools properly apply their scientific knowledge, skill, experience, training and/or education. They should also use a methodology that is reliable within defined standards to show the history, pedigree and reliability of the tools, proper testing and calibration of those tools, and their application to functions they perform within the limitations of their reliable application.

Non-experts can make statement about evidence to the extent that they can clarify non-scientific issues by stating what they observed. Digital forensics evidence can be challenged by establishing that, by intent or accident, content, context, meaning, process, relationships, ordering, timing, location, corroboration and/or consistency are made or missed by the other side, and that this produced false positives or false negatives in the results presented by the other side. The trier of fact then must determine how the evidence is applied to the matter at hand so as to weigh it against and in conjunction with all of the other evidence and to render judgments about the legal matters that the evidence applies to.

Box 7.8 Forensics Experts – What do they Do?

The role of forensics experts has become a very special one in digital forensics and there are many reasons for it. Handling of digital evidence requires special expertise that comes from training and experience. A lot of protocols come into picture depending on the nature of the evidence; for example, the complexity, volume and delicate nature of relevant electronic evidence. Depending on such nature of the evidence, even expensive hardware and software tools will be required along with the investigator's experience to achieve optimal results. In most cases, it is best to address this through partnership with a third party expert forensics firm.

"Peeking around the data" on your own may destroy relevant date and time stamps and other metadata, and more importantly, it may expose you to sanctions for spoliation. Using overly generic discovery requests ("please provide all electronic data") can produce excessively broad or burdensome requests. The court may reject such request as it may be too expensive and time consuming to fulfill these requests. If digital forensics evidence is properly managed, then a computer forensics expert will be able to focus on the relevant electronic discovery targets, and will be able to lower the eventual cost of litigation and increase the probability of a favorable outcome.

A forensics expert team brings the following additional benefits:

1. **Technology expertise:** This is perhaps the biggest advantage of partnership with a computer forensics expert. As an example of the technological complexity, consider the proliferation of operating systems in the last decade: mainframe operating systems, Windows 95/98, UNIX, Linux, Windows NT, Windows Server, Macintosh, Windows 2000, Windows XP and Novell Netware. Specific forensics tools must be used with each of these file systems, along with training and experience to interpret search results. Although some evidence may be found easily, other evidence may have been deleted, altered, hidden or encrypted. Forensics experts routinely deal with such complexities and nuances.
2. **Forensics methodology:** A comprehensive forensics methodology, repeatable and defensible, has become a key attribute in choosing a forensics expert firm. Proper use of a repeatable process prevents making the same mistake twice, ensures proper chain of custody, leverages successful techniques from prior cases, supports clear and concise testimony, and generally guarantees efficient forensics case management.
3. **Experience and efficiency:** The tools and methods of computer forensics examination are still in their infancy. Experts know how to quickly navigate through the variety of esoteric tools and procedures. Experts also have the experience to cull thousands of files based on patterns and keywords. Therefore, working with experts will efficiently produce relevant results for counsel.

The "chain of custody" concept, too, is a very important one in digital forensics (see Section 7.8). We have provided links in Ref. #2, Video Clips, Further Reading about evidence seizure as part of forensics investigation.

Once the forensics experts know the landscape of the computers and other artifacts involved, they formulate a cost proposal governing all needed activities in the forensics search and analysis. This is combined with a proposed timeline of activities, lists of anticipated deliverables and a plan for production and turnover of evidence. In addition to this, forensics experts also submit a preliminary risk analysis for the forensics service being proposed. This will detail any technical and political obstacles that were envisaged. For forensics findings of any type to be used as admissible evidence in court, the data acquisition, also known as "imaging," of the subject computers must be flawless and defensible in substance and technique. Forensics examiners are trained to follow a carefully developed set of protocols for acquisition of electronic evidence designed to ensure authenticity and diligent chain of custody.

7.7.2 The Phases in Computer Forensics/Digital Forensics

The investigator must be properly trained to perform the specific kind of investigation that is at hand. Tools that are used to generate reports for court should be validated. There are many tools to be used in the process.

One should determine the proper tool to be used based on the case. Broadly speaking, the forensics life cycle involves the following phases:

1. Preparation and identification;
2. collection and recording;
3. storing and transporting;
4. examination/investigation;
5. analysis, interpretation and attribution;
6. reporting;
7. testifying.

To mention very briefly, the process involves the following activities:

1. **Prepare:** Case briefings (see Box 7.9), engagement terms, interrogatories, spoliation prevention, disclosure and discovery planning, discovery requests.
2. **Record:** Drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.
3. **Investigate:** Triage images, data recovery, keyword searches, hidden data review, communicate, iterate.
4. **Report:** Oral vs. written, relevant document production, search statistic reports, chain of custody reporting, case log reporting.
5. **Testify:** Testimony preparation, presentation preparation, testimony.

Let us take a brief look at each of the activites mentioned. Table 7.5 shows phase-wise outcome from the phases mentioned above.

Preparing for the Evidence and Identifying the Evidence

In order to be processed and applied, evidence must first be identified as evidence. It can happen that there is an enormous amount of potential evidence available for a legal matter, and it is also possible that the vast majority of the potential evidence may never get identified. Consider that every sequence of events within a single computer might cause interactions with files and the file systems in which they reside, other processes and the programs they are executing and the files they produce and manage, and log files and audit trails of various sorts. In a networked environment, this extends to all networked devices, potentially all over the world. Evidence of an activity that caused digital forensics evidence to come into being might be contained in a time stamp associated with a different program in a different computer on the other side of the world that was offset from its usual pattern of behavior by a few microseconds. If the evidence cannot be identified

Box 7.9 \ Case Briefings

In case briefings, consider the following:

1. Ensure that you know both your client's and the adverse party's position, and have seen all relevant paperwork.
2. Try not to project a bias in the case description; the intent should be to consider the case objectively, and provide you with the good news and the bad news (bad news early can be good news).
3. Be upfront in discussing any limitations or restrictions on the forensics investigation, including budgetary constraints, time deadlines, cooperation levels to be expected from the adverse party, required travel, onsite or after-hours forensics imaging requirements, etc.

as relevant evidence, it may never be collected or processed at all, and it may not even continue to exist in digital form by the time it is discovered to have relevance.

Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. Obvious sources include computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices and so on. Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change). Special care must be taken when handling computer evidence: most digital information is easily changed, and once changed it is usually impossible to detect that a change has taken place (or to revert the data back to its original state) unless other measures have been taken. For this reason, it is common practice to calculate a cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified as the hash was calculated. Figures 7.6 and 7.7 show the media that typically holds digital evidence.



Figure 7.6 Media that can hold digital evidences.

Sources: <http://www.homeofficebuddy.com>; <http://oldcomputers.net>; <http://www.homecomputertalk.com>; <http://www.cyberindian.net>; <http://www.srs-electronicmall.com>; <http://transcriptdivas.co.uk> and <http://images.google.co.in>; <http://www.mobileshop.com>; <http://images.google.co.in>; <http://www.slipperybrick.com>; <http://images.google.co.in>; <http://www.letsgodigital.org>; <http://www.computerrepairmaintenance.com>; <http://www.indigoshop.co.uk>; <http://www.adorama.com>, <http://sp.sony-europe.com/media/4/1914>, <http://www.video99.co.uk/dat.jpg>



Figure 7.7 | Some more media that can hold digital evidences.

Collecting volatile data requires special technical skills. If the machine is still active, any intelligence that can be gained by examining the applications currently open is recorded. If the machine is suspected of being used for illegal communications, such as terrorist traffic, not all of this information may be stored on the hard drive. If information stored solely in random access memory (RAM) is not recovered before powering down, it may be lost. This results in the need to collect volatile data from the computer at the onset of the response.

Embedded flash memory falls under the family of solid state non-volatile memory; it is used in thumb drives (USB stick), cell phones, game console, secure digital cards (SD cards) and multimedia cards (MMC). This technology differs from the normal hard disk by not containing any moving parts such as arms and cylinders. In addition, the physical size of the embedded memory chips makes it a good candidate to be used in every device that interacts with our daily life. The benefits of embedded memory continue to increase life expectancy of the memory chip due to a reduction of mechanical failure even if it had been used in high vibrated or trembling environment. Figure 7.8 shows the various types of “embedded memories” inside a computer (ROM, PROM, EPROM, EEPROM).

Storing and Transporting Digital Evidence

The following are specific practices that have been adopted in the handling of digital evidence:

1. Image computer media using a write-blocking tool to ensure that no data is added to the suspect device;
2. establish and maintain the chain of custody (refer to Section 7.8);

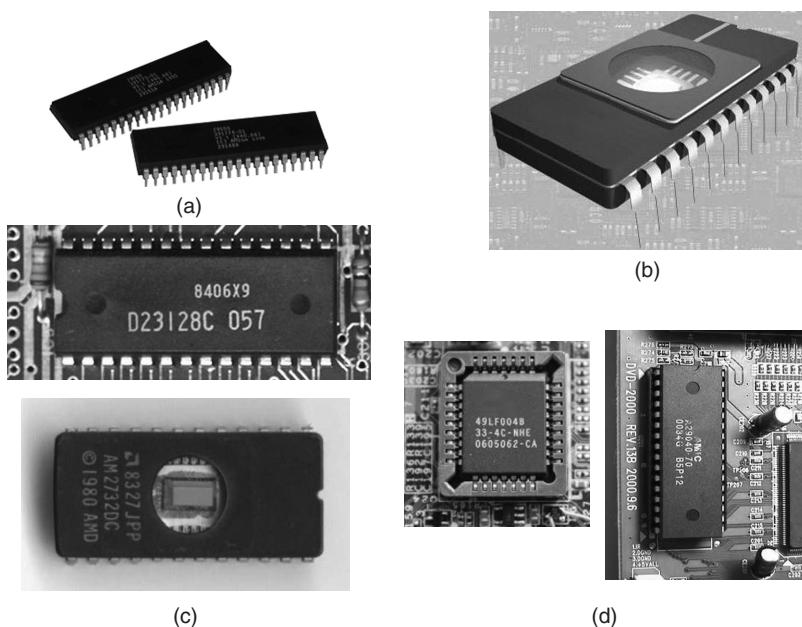


Figure 7.8 Embedded memories inside computer. (a) Read-only memory (ROM) chips; (b) erasable programmable read-only memory (EPROM) chip; (c) programmable read-only memory (PROM) chips; (d) electrically erasable programmable read-only memory (EEPROM) chips. Sources: <http://amigakit.leanmancomputing.com>; <http://www.old-computers.com>; <http://upload.wikimedia.org> and <http://www.electrongate.com>; <http://wiki.laptop.org> and <http://www.dv-rec.de>

3. document everything that has been done;
4. only use tools and methods that have been tested and evaluated to validate their accuracy and reliability.



Some of the most valuable information obtained in the course of a forensics examination will come from the computer user. An interview with the user can yield valuable information about the system configuration, applications, encryption keys and methodology. Forensics analysis is much easier when analysts have the user's passphrases to access encrypted files, containers and network servers.

In storage, digital media must be properly maintained for the period of time required for the purposes of trial. Depending on the particular media (see Figs. 7.6 and 7.7), this may involve any number of requirements ranging from temperature and humidity controls to the need to supply additional power or to re-read media. Storage must be adequately secure to assure proper "chain of custody" (refer to Section 7.8), and typically, for evidence areas containing large volumes of evidence, paperwork associated with all actions related to the evidence must be kept to assure that evidence does not go anywhere without being properly traced. Many things can go wrong in storage, including decay over time; environmental changes resulting in the presence or absence of a necessary condition for preservation; direct environmental assault on the media; fires, floods and other external events reaching the evidence; loss of power to batteries and other media-preserving mechanisms; and decay over time from other natural and artificial sources.

Sometimes evidence must be transported from place to place. For example, when collected from a crime scene, the evidence must somehow be moved to a secure location or it may not be properly preserved through a trial. Digital forensics evidence can generally be transported by making exact duplicates, at the level of bits, of the original content. This includes the movement of content over networks, assuming adequate precautions are taken to assure its purity during that transportation.

Evidence is often copied and sent electronically, on compact disks or on other media, from place to place. Original copies are normally kept in a secure location to act as the original evidence that is introduced into the legal proceedings. If there is any question about the bits contained in the evidence, it can be settled by returning to the original evidence. Facsimile evidence, printouts and other similar depictions of digital forensics evidence may also be transported, but they are not a good substitute for the original digital forensics evidence in most cases, among other reasons, because they make it far harder, if not impossible, to properly analyze what the original bits were. For example, many different bit sequences may produce the output depictions, and identical bit sequences may produce different output depictions.

Adequate care must be taken in transportation to prevent spoliation as well. For example, in a hot car, digital media tends to lose bits. Increasingly, evidence is transported electronically from place to place, and even the simplest errors can cause the data arriving to be incorrect or improperly authenticated for legal purposes. Care must also be taken to preserve chain of custody and assure that a witness can testify accurately about what took place, using and retaining contemporary notes, and taking proper precautions to assure that evidence is not spoilt and is properly treated along the way.

Examining/Investigating Digital Evidence

In an investigation in which the owner of the digital evidence has not given consent to have his or her media examined (as in some criminal cases) special care must be taken to ensure that the forensics specialist has the legal authority to seize, copy and examine the data. Sometimes authority stems from a search warrant.



As a general rule, one should not examine digital information unless one has the legal authority to do so. Amateur forensics examiners should keep this in mind before starting any unauthorized investigation.

Now let us understand the difference between live and dead analysis. After that we explain about “imaging of the media.” Traditionally, computer forensics investigations were performed on data at rest, for example, the content of hard drives. This can be thought of as a “dead analysis.” Investigators were told to shutdown computer systems when they were impounded for fear that digital time bombs might cause data to be erased. In recent years, there has been increasingly an emphasis on performing analysis on live systems. One reason is that many current attacks against computer systems leave no trace on the computer’s hard drive; the attacker only exploits information in the computer’s memory. Another reason is the growing use of cryptographic storage: it may be that the only copy of the keys to decrypt the storage is in the computer’s memory; turning OFF the computer will cause that information to be lost.



For the purpose of digital evidence examination, “imaging of electronic media” (on which the evidence is believed to be residing) becomes necessary.

The process of creating an exact duplicate of the original evidentiary media is often called “Imaging.” Computer forensics software packages make this possible by converting an entire hard drive into a single searchable file – this file is called an “image.” Using a stand-alone hard drive duplicator or software imaging tools such as DCFLdd, IXImager or Guymager, the entire hard drive is completely duplicated. This is usually done at the sector level, making a bit-stream copy of every part of the user-accessible areas of the hard drive which can physically store data, rather than duplicating the file system. The original drive is then moved to secure storage to prevent tampering. During imaging, a write protection device or application is normally used to ensure that no information is introduced onto the evidentiary media during the forensics process. The imaging process is verified by using the SHA-1 message digest algorithm (with a program such as sha1sum) or other still viable algorithms such as MD5. At critical points throughout the analysis, the media is verified again, known as “hashing,” to ensure that the evidence is still in its original state. In corporate environments seeking civil or internal charges, such steps are generally overlooked due to the time required to perform them. They are essential for evidence that is to be presented in a courtroom, however.

Analysis, Interpretation and Attribution

Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics analysts. In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence; however, the actual number of possible sequences may be almost unfathomably large. In essence, almost any execution of an instruction by the computing environment containing or generating the evidence may have an impact on the evidence. Basically, all digital evidence must be analyzed to determine the type of information that is stored upon it. For this purpose, specialty tools are used that can display information in a format useful to investigators. Such forensics tools include but are not limited to the following list. Readers can refer to links in References to know more about this toolkit. (Also refer to Appendix I in CD.)

1. Access Data’s FTK^[2];
2. guidance Software’s EnCase^[3];
3. Dr. Golden Richard III’s file carving tool Scalpel^[4]; “file carving” is the process of recovering files from an investigative target, potentially without knowledge of the file system structure;
4. Brian Carrier’s Sleuth Kit^[5]: The Sleuth Kit (TSK) is a library and collection of Unix- and Windows-based tools and utilities to allow for the forensics analysis of computer systems.

Typical forensics analysis includes a manual review of material on the media – an example of OS-specific investigation is reviewing the Windows registry. Through this registry inspection, the investigators objective is to look for suspect information, discovering and cracking passwords, performing keyword searches for topics related to the crime, and extracting E-Mail and images for review. Numerous other tools are used in digital forensics investigations to analyze specific portions of information. See Box 7.10 regarding file carving technique. In Chapter 11 (Section 11.6.2), we have provided case studies based on TSK and EnCase.

Box 7.10 File Carving – a Powerful Technique for Digital Forensics

File carving is the process of recovering files from an investigative target, potentially without knowledge of the file system structures. The process is based on information about the format of the file types of interest, as well as on assumptions about how files are typically laid out on block devices. If the file system metadata is used at all, it is typically used only for establishing cluster sizes and avoiding carving of undeleted files (which can be extracted without file carving).

Box 7.10 File Carving . . . (Continued)

File carving is an important technique for digital forensics investigation and for simple data recovery. By using a database of headers and footers (essentially, strings of bytes at predictable offsets) for specific file types, file carvers can retrieve files from raw disk images, regardless of the type of file system on the disk image. Perhaps more importantly, file carving is possible even if the file system metadata has been destroyed. File carving is a particularly powerful technique because files can be retrieved from raw disk images, regardless of the type of file system. File retrieval is possible even if the file system metadata has been completely destroyed. For example, a file deposited on a FAT partition can often be recovered even if the partition is reformatted as NTFS, then ext2, then FAT again, even if bad block checks (which are generally read-only operations) are applied. Although a file system's metadata can be quite fragile, file data is much more resilient. One limitation of the current generation of automatic file carvers is that a file's data must be contiguous to be carved properly.

With some manual intervention or additional work, even non-contiguous data can be carved. Luckily, modern file systems, such as ext2/3 (for Linux) and NTFS (for Windows), are actually quite kind to file carvers. This is because they strive to perform disk allocation which minimizes file fragmentation to reduce seek time and improve file system performance. Even under legacy file systems such as FATx, which are prone to fragmentation, the data of many files of modest size is likely to be unfragmented. This is because file fragmentation, if present, is on cluster boundaries and cluster sizes under FATx tend to be rather large.

File carvers ignore the file system and carve the images directly from data blocks. In cases of fragmented files, the carver returns an imperfect photo, but this image might be sufficient to identify the subject (see Fig. 7.9).

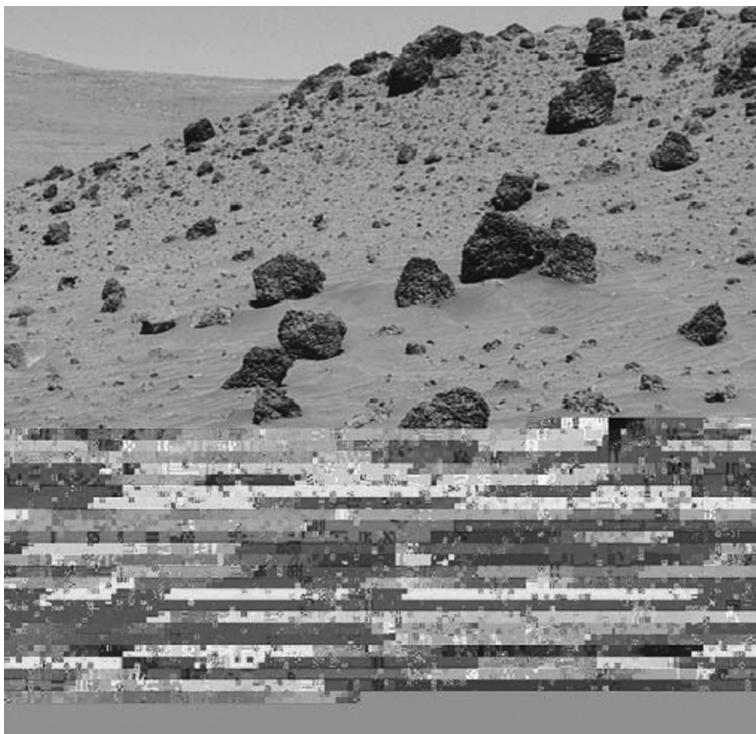


Figure 7.9 An image constructed from a fragmented file.
Source: Linux Magazine available at the link: http://www.linux-magazine.com/w3/issue/93/Foremost_Web.pdf (24 December 2009).

As it is not feasible to reconstruct every possible sequence to investigate all the sequences that may have produced the actual evidence in any particular case, forensics analysts focus only on large sets of sequences of events. They tend to characterize evidence aspects in those terms. For example, if the evidence includes a log file that appears to be associated with a file transfer, the name of the file transfer program included in the log file will typically be associated with common behavior of that program and will be used as a basis for the analysis (readers will understand this when they refer to cyberforensics investigation case – Digital Forensics Case Illustration 2: Analysis of Seized Floppy – the Drug Peddler Case in Section 11.6.2 of Chapter 11). The user identity indicated in the log file may be associated with a human or group, and this creates an initial attribution that can then be used as a basis for further efforts to attribute to the standard of proof required. Note, however, that the presence of this record in an audit trail does not mean that the program was ever run at all or that the thing the record indicates ever took place or that the user identified caused the events of interest. There are many possible sequences of events that could result in the presence of such a record. For example, without limiting the totality of possible event sequences, the record could have been placed there maliciously; it could be a record produced by another program that looks similar to the program being considered; it could have been a record produced by the program even though the file transfer failed; the record could have been produced by a Trojan Horse acting for the user or the record could be there because of a failure in a disk write that produced a crosslink between disk blocks associated with different sorts of records.

Analysis, interpretation and attribution of digital forensics evidence can be reconciled with non-digital evidence and digital forensics evidence can be externally stipulated or they can be demonstrated facts. For example, suppose the digital forensics evidence appears to show that person X was present at the local console of a computer in Los Angeles, California, two hours after passing through customs and immigration in London, UK. Suppose further that the network logs from distant systems show that the transfer indeed took place; even then, it is not a reasonable interpretation to assert that the individual was in Los Angeles. Another explanation is possible, whether there are two distinct individuals involved rather than a single individual, a remote control mechanism, alteration of multiple logs in multiple systems, alteration of customs and immigration logs, altered time clocks or any of a long list of other possibilities. Although in some venues, the “do not confuse me with the facts” approach may apply, in a legal setting, digital forensics evidence should reconcile with external reality.

Several open-source tools are available to conduct an analysis of open ports, mapped drives (including through an active VPN connection) and open or mounted encrypted files (containers) on the live computer system. Utilizing open-source tools and commercially available products, it is possible to obtain an image of these mapped drives and the open encrypted containers in an unencrypted format. Open-source forensics tools^[6] for PCs include Knoppix and Helix by US e-fense Inc. These are Unix-based tools used in Linux environment. Commercial imaging tools include Access Data's Forensics Toolkit and Guidance Software's EnCase application.

The above-mentioned open-source tools mentioned can also scan RAM and Registry information to show recently accessed Web-based E-Mail sites and the login/password combination used. Additionally, these tools can also yield login/password for recently accessed local E-Mail applications including MS Outlook. In the event that partitions with Encrypted File System (EFS – file system driver that provides filesystem-level encryption in Microsoft Windows operating systems) are suspected to exist, the encryption keys to access the data can also be gathered during the collection process. With Microsoft's most recent addition, Vista and Vista's use of BitLocker and the Trusted Platform Module (TPM), it has become necessary in some instances to image the logical hard drive volumes before the computer is shutdown.

RAM can be analyzed for prior content after power loss. Although as production methods become cleaner, the impurities used to indicate a particular cell's charge prior to power loss are becoming less common. However, data held statically in an area of RAM for long periods of time are more likely to be detectable using these methods. The likelihood of such recovery increases as the originally applied voltages,

operating temperatures and duration of data storage increases. Holding unpowered RAM below -60°C will help preserve the residual data by an order of magnitude, thus improving the chances of successful recovery. However, it is impractical to do this during a field examination.

Now let us understand *types of digital analysis*. It is important, because, a digital investigation may encounter many formats of digital data and, therefore, there exist several types of analysis. The different analysis types are based on interpretation, or abstraction, layers, which are generally part of the data's design. For example, consider the data on a hard disk, which has been designed with several interpretation layers. The lowest layer may contain partitions or other containers that are used for volume management. Inside each partition is data that has been organized into a file system or database. The data in a file system is interpreted to create files that contain data in an application-specific format. Each of these layers has its own analysis techniques and requirements. Examples of common digital analysis types include:

Box 7.11 The RAID Levels

Explanation of RAID is important in forensics context. RAID data acquisitions are performed as part of computer forensics. RAID stands for Redundant Array of Independent (or inexpensive) Disks. It is a category of disk drives that employs multiple drives in combination for fault tolerance and performance. Although use of RAID disk drives is frequent on servers, the use is not generally necessary for personal computers. With RAID, you can store the same data redundantly, that is, in multiple places in a balanced way to improve overall performance. In late 1980s and early 1990s, computer information servers had to sustain a dramatic increase in capacity expectation in terms of amount of data served and stored on them. Storage technologies had become too expensive to place a large number of high-capacity hard drives in the servers. The response to this situation came through concept of RAID; subsequently RAID became very popular. Note that "data striping" means spreading out blocks of each file across multiple disk drives.

RAID was a system developed as a solution to link together a large number of low-cost hard drives with a view to form a single large capacity storage device that provided superior performance, storage capacity and reliability as compared to older storage solutions. Since then RAID became widely used and is deployed as an enterprise storage method in server markets. However, in the last 5 years it has become much more common in end-user systems.

Attractiveness of RAID comes from the fact that the array of disks distributes data across multiple disks; however, computer user and operating system sees the array as one single disk. The array of disks (RAID) can be set up to serve multiple purposes and offers many advantages such as redundancy, increased performance and lower costs.

Those who are technically savvy may know that there are number of different RAID levels as follows:

1. **Level 0:** This is nothing but a striped disk array without fault tolerance. It provides data striping (spreading out blocks of each file across multiple disk drives) but no redundancy. This results in an improved performance; however, it does not deliver fault tolerance. All data in the array is lost if one drive fails.
2. **Level 1:** This is mirroring and duplexing to provide disk mirroring. Level 1 provides double the rate of read transaction for single disks, but provides the same write transaction rate as single disks.
3. **Level 2:** This is error-correcting coding; however, it is not a typical implementation. This level is rarely used. It stripes data at the bit level rather than the block level.
4. **Level 3:** This is bit-interleaved parity. Level 3 provides byte-level striping with a dedicated parity disk. It is rarely used; probably because it cannot service simultaneous multiple requests.
5. **Level 4:** This is dedicated parity drive. Its use is common for implementation of RAID. Level 4 offers block-level striping (like Level 0) with a parity disk. If a data disk fails, the parity data is used to create a replacement disk. There is a disadvantage to Level 4 in that the parity disk can create write bottlenecks.

Box 7.11 The RAID . . . (Continued)

6. **Level 5:** This is block interleaved distributed parity. The idea here is to provide data striping at the byte level and also to stripe error correction information. Level 5 results in excellent performance and good fault tolerance. It is most popular among RAID implementation methods.
7. **Level 6:** This is independent data disks with double parity. This level provides block-level striping with parity data distributed across all disks.
8. **Level 0+1:** This is nothing but a mirror of stripes. It is not one of the original RAID levels. With this level used, two RAID 0 stripes are created and one RAID 1 mirror is created over them. The use of this level is typically seen for both replicating and sharing data among disks.
9. **Level 10:** This is stripe of mirrors. However, it is not considered to be an original RAID level. With this level, multiple RAID 1 mirrors are created, and a RAID 0 stripe is created over these.
10. **Level 7:** This is a trademark of STC (Storage Computer Corporation). It adds caching to Levels 3 or 4.
11. **RAID S:** This is also known a Parity RAID. It is an EMC Corporation's proprietary striped parity RAID system used in its Symmetrix storage systems.

For desktop computer systems, there are typically three forms of RAID used: RAID 0, RAID 1 and RAID 5.

1. **Media analysis:** It is analysis of the data from a storage device. This analysis does not consider any partitions or other operating system (OS)-specific data structures. If the storage device uses a fixed size unit, such as a sector, then it can be used in this analysis.
2. **Media management analysis:** It is analysis of the management system used to organize media. This typically involves partitions and may include volume management or redundant array of independent (or inexpensive) disks (RAID, see Box 7.11) systems that merge data from multiple storage devices into a single virtual storage device.
3. **File system analysis:** It is the analysis of the file system data inside a partition or disk. This typically involves processing the data to extract the contents of a file or to recover the contents of a deleted file.
4. **Application analysis:** It is the analysis of the data inside a file. Files are created by users and applications. The format of the contents is application-specific.
5. **Network analysis:** It is the analysis of data on a communications network. Network packets can be examined using the OSI Model to interpret the raw data into an application-level stream. Application analysis is a large category of analysis techniques because there are many application types. Some of the most common ones are as follows:
 - *OS analysis:* An OS is an application, although it is a special application because it is the first one that is run when a computer starts. This analysis examines the configuration files and output data of the OS to determine what events may have occurred.
 - *Executable analysis:* Executables are digital objects that can cause events to occur and they are frequently examined during intrusion investigations because the investigator needs to determine what events the executable could cause.
6. **Image analysis:** It was mentioned that the “image” is a single searchable file. Digital images are the target of many digital investigations because some are contraband. This type of analysis looks for information about where the picture was taken and who or what is in the picture. Image analysis also includes examining images for evidence of steganography (steganography in the context of forensics is discussed in Section 7.12).
7. **Video analysis:** Digital video is used in security cameras and in personal video cameras and webcams. Investigations of online predators can sometimes involve digital video from webcams. This type of analysis examines the video for the identification of objects in the video and the location where it was shot.

Reporting

Once the analysis is complete, a report is generated. The report may be in a written form or an oral testimony or it may be a combination of the two. Finally, evidence, analysis, interpretation and attribution must ultimately be presented in the form of expert reports, depositions and testimony. After extracting and analyzing the evidence collected, the results may need to be presented before a wide variety of audience including law enforcement officials, technical experts, legal experts, corporate management, etc. Depending on the nature of the incident or crime, it may become mandatory to present the findings in a court of law. It could be a police investigation or a presentation to appropriate corporate management or it could be an internal company investigation. As a result of the findings in this phase, it should be possible to confirm or discard the allegations with regard to particular crime or suspected incident. The presentation of evidence and its analysis, interpretation and attribution have many challenges.

Presentation of the report is more of an art than a science, but there is a substantial amount of scientific literature on methods of presentation and their impact on those who observe those presentations. Aspects ranging from the order of presentation of information to the use of graphics and demonstrations, all present significant challenges and are poorly defined. In general, reporting is a complex and tricky process and beyond the scope of discussion here. The following are the broad-level elements of the report:

1. Identity of the reporting agency;
2. case identifier or submission number;
3. case investigator;
4. identity of the submitter;
5. date of receipt;
6. date of report;
7. descriptive list of items submitted for examination, including serial number, make and model;
8. identity and signature of the examiner;
9. brief description of steps taken during examination, such as string searches, graphics image searches and recovering erased files;
10. results/conclusions.

In Chapter 11, we present illustrative examples of a digital forensics investigation report (refer to Section 11.6.3).

Testifying

This phase involves presentation and cross-examination of expert witnesses. Depending on the country and legal frameworks in which a cybercrime case is registered, certain standards may apply with regard to the issues of expert witnesses. Digital forensics evidence is normally introduced by expert witnesses except in cases where non-experts can bring clarity to non-scientific issues by stating what they observed or did. For example, a non-expert who works at a company may introduce the data he/she extracted from a company database and discuss how the database works and how it is normally used from a non-technical standpoint. To the extent that the witness is the custodian of the system or its content, he/she can testify to matters related to that custodial role as well.

Only expert witnesses can address issues based on scientific, technical or other specialized knowledge. A witness qualified as an expert by knowledge, skill, experience, training or education may testify in the form of an opinion or otherwise if (a) the testimony is based on sufficient facts or data, (b) the testimony is the product of reliable principles and methods, and (c) the witness has applied the principles and methods reliably to the facts of the case. If facts are reasonably relied upon by experts in forming opinions or inferences, the facts need not be admissible for the opinion or inference to be admitted; however, the expert may in any event be required to disclose the underlying facts or data on cross-examination.



Experts typically have very specialized knowledge about specific things of import to the matter at hand and anyone put up as an expert who does not have the requisite specialized knowledge can be seriously challenged by competent experts and counsel on the other side. Experts who are shown to be inadequate to the task are sometimes chastised in the formal decisions made by the courts, and such witnesses are often unable to work in the field for a period of many years thereafter because counsel for the opposition will bring this out at trial.

Now that we have explained the phases involved in the digital forensics investigation process, to conclude this section, we have summarized in Table 7.5 the outcomes from those phases. After that we have explained about precautions to be taken while collecting electronic evidence.

7.7.3 Precautions to be Taken when Collecting Electronic Evidence

So far we have established how important the digital/computer evidence is for cyberforensics. Therefore, collection of the evidence must happen with due care. Special measures should be taken while conducting a forensics investigation if it is desired for the results to be used in a court of law. One of the most important

Table 7.5 | Digital forensics – phase-wise outputs

Phase	Activities/Processes	Outputs
Evidence		Plan
Preparation and Identification	<ul style="list-style-type: none"> • Monitoring authorization and management support, and obtain authorization to do the investigation. • Ensuring that operations and infrastructure are able to support an investigation. • Providing a mechanism for the incident to be detected and confirmed. • Creating an awareness so that the investigation is needed (identify the need for an investigation). • Planning for getting the information needed from both inside and outside the investigating organization. • Identifying the strategy, policies and previous investigations. • Informing the subject of an investigation or other concerned parties that the investigation is taking place. 	Authorization Warrant Notification Confirmation
Collection and Recording	<ul style="list-style-type: none"> • Determine what a particular piece of digital evidence is, and identifying possible sources of data. • Determine where the evidence is physically located. • Translating the media into data. 	Crime type Potential Evidence Sources
Preserving and Transportation	<ul style="list-style-type: none"> • Ensuring integrity and authenticity of the digital evidence, for example, write protection, hashes, etc. • Packaging, transporting and storing the digital evidence. • Preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius. • Recording the physical scene. • Duplicating digital evidence using standardized and accepted procedures. • Ensuring the validity and integrity of evidence for later use. 	Media Devices Event

(Continued)

Table 7.5 | (Continued)

<i>Phase</i>	<i>Activities/Processes</i>	<i>Outputs</i>
<i>Examination/ Investigation and Analysis,</i>	<ul style="list-style-type: none"> Determining how the data is produced, when and by whom. Determine and validating the techniques to find and interpret significant data. 	Log files, file Events log Data
<i>Interpretation and Attribution</i>	<ul style="list-style-type: none"> Extracting hidden data, discovering the hidden data and matching the pattern. Recognizing obvious pieces of digital evidence and assessing the skill level of suspect. Transform the data into a more manageable size and form for analysis. Confirming or refuting allegations of suspicious activity. Identifying and locating potential evidence, possibly within unconventional locations. Constructing detailed documentation for analysis and drawing conclusions based on evidence found. Determining significant based on evidence found. Testing and rejecting theories based on the digital evidence. Organizing the analysis results from the collected physical and digital evidence. Eliminating duplication of analysis. Build a timeline. Constructing a hypothesis of what occurred, and comparing the extracted data with the target. Documenting the findings and all steps taken. 	Information
<i>Presentation and reporting</i>	<ul style="list-style-type: none"> Preparing and presenting the information resulting from the analysis phase. Determine the issues relevance of the information, its reliability and who can testify to it. Interpreting the statistical from analysis phase. Clarifying the evidence and documenting the findings. Summarizing and providing explanation of conclusions. Presenting the physical and digital evidence to a court or corporate management. Attempting to confirm each piece of evidence and each event in the chain either along with each other, or independent of one evidence and/or other events. Proving the validity of the hypothesis and defend it against criticism and challenge. Communicating relevant findings to a variety of audiences (management, technical personnel, law enforcement). 	Evidence, Report
<i>Disseminating the case</i>	<ul style="list-style-type: none"> Ensuring physical and digital property is returned to proper owner. Determining how and what criminal evidence must be removed. Reviewing the investigation to identify areas of improvement. Disseminating the information from the investigation. Closing out the investigation and preserving knowledge gained. 	Evidence Explanation New policies and investigation Procedures Evidence disposed Investigation closed

measures is to ensure that the evidence has been accurately collected and that there is a clear chain of custody right from the scene of the crime to the investigator and ultimately to the court (the “chain of custody” concept is explained in Section 7.8 – see Box 7.4 and Box 7.12).

In order to comply with the need to maintain the integrity of digital evidence, certain rules must be complied with. In general, the following principles are applicable:

1. **Principle 1:** No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.
2. **Principle 2:** In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media that person must be competent to do so and be able to give evidence explaining the relevance and the implications of his/her actions.
3. **Principle 3:** An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. **Principle 4:** The person in-charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

7.8 Chain of Custody Concept



Chain of custody is the central concept in cyberforensics/digital forensics investigation.

Recall the discussion we had in Section 7.4 and Box 7.4. A chain of custody is the process of validating how many kinds of evidences have been gathered, tracked and protected on the way to a court of law. It is essential to get in the habit of protecting all evidences equally so that they will hold up in court. Forensic investigation professionals know that if you do not have a chain of custody, the evidence is worthless. They learn to deal with everything as if it would go to litigation.



The purpose of the chain of custody is that the proponent of a piece of evidence must demonstrate that it is what it purports to be.

In other words, there is a reliable information to suggest that the party offering the evidence can demonstrate that the piece of evidence is actually, in fact, what the party claims it to be and can further demonstrate its origin and the handling of the evidence because it was acquired.



The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition until its final disposition.

A chain of custody begins when an item of relevant evidence is collected, and the chain is maintained until the evidence is disposed off (Figs. 7.10 and 7.11). The chain of custody assumes continuous accountability. This accountability is important because, if not properly maintained, an item (of evidence) may be inadmissible in court.

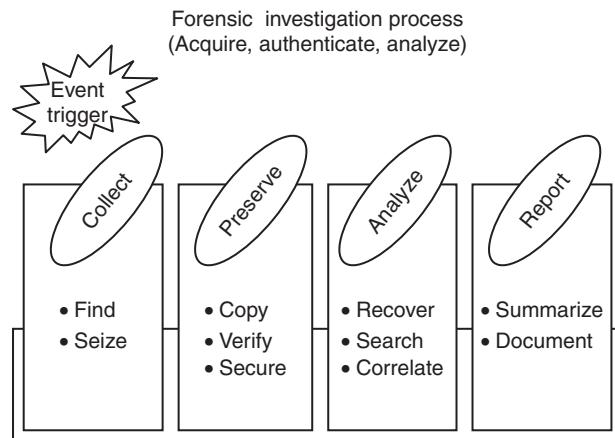


Figure 7.10 | Maintaining chain of custody – 1.

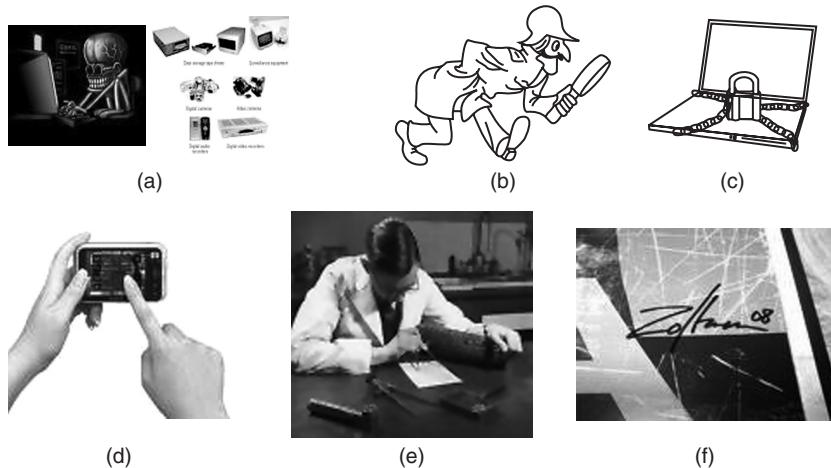


Figure 7.11 | Maintaining chain of custody – 2. (a) Source of evidence – where did it come from? (b) Who found it? (c) Where was it stored/locked up? (d) Who touched it/tampered with it? (e) What did they do to it? What did they do with it? (f) Human signature is always required.

Box 7.12 The Chain of Evidence Concept

A trial can be lost quickly if opposing counsel can show that the evidence chain of custody was violated. Before the world became computerized, proving chain of custody was easier. Attorneys and law enforcement filled out a chain of custody form that showed who had handled the evidence and the dates and times. With so much evidence coming from computers, especially in civil cases, many law firms need chain of custody software that is foolproof.

Box 7.12 The Chain . . . (Continued)

To avoid the risk of mishandling evidence, proper chain of custody procedure should always be strictly observed. This includes a thorough documentation of sources of data, the use of "write-blocking" devices to ensure no data changes take place inadvertently; initial forensics screening of disk drives for relevant data and making bit-for-bit copies of hard drives (images). The chain of custody also ensures that digital fingerprints (file hashes) match up at all stages of investigation, and that documentation (including photography and serial number inventory) of all evidence artifacts, as well as maintaining case logs for all evidence-related activities, is performed.

When preparing for trial, you need reliable chain of custody software supported by experts that know the latest rules. From the time we receive the media to the time we ship the results back, chain of custody is upheld. In a forensics data recovery, the senior individuals on forensics staff are the only ones who have access to the media. This allows for an efficient recovery and limits amount of individuals who have contact with the evidence.

Collecting information regarding the environment and use of the computer or machine under investigation, in an attempt to answer questions such as the following prior to the arrival of the forensics investigator, should be of utmost importance (refer to Figs. 7.10 and 7.11):

1. Who had access to the machine?
2. What level of authorization did all of those individuals having access to the machine have?
3. What was the machine used for?
4. What external devices did the machine connect to or interact with?
5. Which and how many servers did the machine "touch"?
6. Where and how will you store and safeguard the machine and the evidence after seizure?
7. Will you or an external third party be responsible for the storage and safeguarding of the seized machine and associated evidence?

At the very least, the evidence or property custody document should include the following information:

1. Name or initials of the individual collecting the evidence;
2. each person or entity subsequently having custody of it;
3. dates on which the evidence items were collected or transferred;
4. department (or Agency or Unit or Team) name and case number;
5. a brief description of the item seized.

7.9 Network Forensics

Recall the mention of network forensics in Section 7.5. We have already discussed that open networks can be the source of many network-based cyberattacks. In fact, a recent survey done^[7] by the Cop-Tech forum (a joint initiative of cybercrime cell of police and city IT firms) in a leading IT business city revealed that 50% of the Wi-Fi Internet connection in the city continued to be unprotected! A situation like this leads to the point that network forensics professionals need to understand how wireless networks work and the fundamentals of related technology. The topic of wireless network forensics is too vast and this section is aimed at providing an overview only here – from security perspective, they are the most risky ones. To know more about security of wireless networks, refer to Ref. #18, Books, Further Reading. In 1997, Marcus Ranum coined the term "wireless forensics."



Wireless forensics is a discipline included within the computer forensics science, and specifically, within the network forensics field. The goal of wireless forensics is to provide the methodology and tools required to collect and analyze (wireless) network traffic that can be presented as valid digital evidence in a court of law.

The evidence collected can correspond to plain data or, with the broad usage of VoIP technologies, especially over wireless, can include voice conversations. The wireless forensics process involves capturing all data moving over Wi-Fi network and analyzing network events to uncover network anomalies, discover the source of security attacks and investigate breaches on computers and wireless networks to determine whether they are or have been used for illegal or unauthorized activities. When performing wireless forensics, the security analyst must follow the same general principles that apply to computer forensics: identify, preserve and analyze the evidence to impartially report the findings and conclusions. There are many technical challenges for Wi-Fi traffic acquisition. That discussion is beyond the scope of this chapter. We have provided some useful resources on the topic of wireless network forensics in References Section.^[8]

7.10 Approaching a Computer Forensics Investigation

From the discussion so far, we can appreciate that computer forensics investigation is a detailed science. The main phases are: *secure the subject system* (from tampering during the operation); *take a copy of hard drive* (if applicable); *identification and recovery of files* (including those deleted); *access/copy hidden, protected and temporary files*; *study “special” areas on the drive* (e.g., residue from previously deleted files); *investigate data/settings from installed applications/programs*; *assess the system as a whole, including its structure*; *consider general factors relating to the user’s activity*; *create detailed report*. Throughout the investigation, it is important to stress that a full audit log of your activities should be maintained. In Chapter 12 (in CD), there is guidance on the topics of building career in cybersecurity.

Cyberforensics experts go by their experience which shows that computer criminals always leave tracks (Locard’s Exchange Principle – Box 7.5); it is just a matter of finding these tracks. However, this is not always easy. Computer technology is continuously evolving. Computers and other communication systems are becoming very complex. People businesses and organizations are connected through all kinds of networks. At the same time, computer crime techniques are becoming more sophisticated and better coordinated (refer to Chapter 4 – Tools and Methods Used in Cybercrime). If evidence collection is done correctly, it is much more useful in apprehending the attacker and stands a much greater chance of being admissible in the event of a prosecution.

Now, let us understand how a forensics investigation is typically approached and the broad phases involved in the investigation. The phases involved are as follows:

1. Secure the subject system (from tampering or unauthorized changes during the investigation);
2. take a copy of hard drive/disk (if applicable and appropriate);
3. identify and recover all files (including deleted files);
4. access/view/copy hidden, protected and temp files;
5. study “special” areas on the drive (e.g., the residue from previously deleted files);
6. investigate the settings and any data from applications and programs used on the system;
7. consider the system as a whole from various perspectives, including its structure and overall contents;
8. consider general factors relating to the user’s computer and other activity and habits in the context of the investigation;
9. create detailed and considered report, containing an assessment of the data and information collected.

Certain things should be avoided during the forensics investigation depending on the nature of the computer system being investigated. For example, one should avoid changing date/time stamps (of files for example) or changing data itself. The same applies to the overwriting of unallocated space (which can happen on reboot for example). “Study it but Do NOT Change” is a useful catch phrase!

While there are some things that should be avoided, there are also other things that cannot be/should not be avoided before taking up a forensics investigation. The engagement contract and non-disclosure agreement (NDA) are some of those crucial not-to-forget things. This is because, customers of computer forensics laboratory must agree to be bound by terms and conditions of service set forth for any services offered by a computer forensics laboratory. In the context of a typical NDA, “customer” means the person, firm or company ordering products or services; “default” means any breach by either party of its obligations or any act, omission, negligence or statement by either party, its employees, agents or subcontractors arising out of or in connection with a contract and in respect of which either party may be legally liable; “the company” means the computer forensics laboratory; “engagement” means any job or jobs assigned to the computer forensics laboratory by the customer.

7.10.1 Typical Elements Addressed in a Forensics Investigation Engagement Contract

Typically, the following important elements are addressed before while drawing up a forensics investigation engagement contract:

- 1. Authorization:** The customer will be asked to authorize the computer forensics laboratory or its agents to conduct an evaluation of the data/media/equipment onsite or offsite to determine the nature and scope of the engagement and to enable the company to provide an estimate of the cost of forensics investigation and/or the turnaround. Furthermore, the customer will be asked to agree on facilitating the engagement by providing all authorizations, security or legal clearances as required prior or throughout the course of the forensics investigation engagement.

The customer will be required to authorize the computer forensics laboratory, its employees, independent contractors and agents to securely receive and transport the media/equipment/data to, from and between their premises required to deliver the services contracted by the customer.

The customer will need to represent, warrant and affirm that he/she, or it is the owner or the authorized representative of the owner of the property or the equipment and all of the information and data stored on said property or equipment. By entering the NDA, the customer is supposed to declare that the representations are true and correct. The customer needs to agree to indemnify concerned computer forensics laboratory for any claims against the company related to any jobs assigned to the computer forensics laboratory whose services are engaged for the forensics investigation.

- 2. Confidentiality:** The concerned computer forensics is supposed to use any information contained in the data, media and/or equipment provided to the company by the customer only for the purpose of fulfilling the engagement, and is expected to hold such customer information in the strictest confidence. Any confidential information disclosed by the customer under the agreement remains the owner's sole property, and computer forensics laboratory shall employ reasonable measures to prevent the unauthorized use of customer information. Such measures shall not be less than those measures employed by computer forensics laboratory in protecting its own confidential information. The involved computer forensics laboratory cannot disclose confidential information except to its employees, consultants or subcontractors as needed for the sole purpose of performing the engagement. Such information is not to be disclosed to any other party except as required by law. Computer forensics laboratory is to employ appropriate technical and organizational measures to safeguard any customer information, including personal data, and will act only on the instruction of the customer with regard to such information.
- 3. Payment:** Customer agrees to pay the computer forensics laboratory all sums authorized from time to time by customer, which will typically include (a) charges for computer forensics laboratory

services; (b) reasonable travel and per diem expenses for onsite work; (c) shipping and insurance and actual expenses, if any, for parts; (d) media and/or off-the-shelf software used in the forensics service engagement. Unless otherwise agreed to in advance by computer forensics laboratory, all such sums are due and payable in advance by company check, bank wire transfer or credit card.

4. **Consent and acknowledgment:** Any consent required of either party becomes effective only if provided in a commercially reasonable manner; this includes but is not limited to, verbal authorization if followed by written confirmation, electronic or otherwise, by the computer forensics laboratory at the earliest possible opportunity. Customer needs to acknowledge that the equipment/data/media may be damaged prior to computer forensics laboratory receipt. Customer also needs to acknowledge that the efforts of the engaged computer forensics laboratory to complete the forensics investigation engagement may result in the destruction of or damage to the equipment/data/media. The computer forensics laboratory will not, however, assume responsibility for additional damage that may occur to the customer's equipment/data/media during computer forensics laboratory efforts to complete the engagement.
5. **Limitation of liability:** The concerned computer forensics laboratory will not consider itself to be liable for any claims regarding the physical functioning of the equipment/media or the condition or existence of data stored on the media supplied before, during or after services. In no event will the forensics laboratory be liable for any loss of data or loss of revenue or profits, goodwill or anticipated savings or any consequential loss whether sustained before, during or after services even if computer forensics laboratory has been advised of the possibility of damages or loss to persons or property.

The customer must be made aware of the inherent risks arising out of possible damage to media or equipment during the course of forensics investigation. Such risks include but are not limited to risks arising from possible destruction or damage to the media or equipment and/or data stored and inability to recover data, or inaccurate or incomplete forensics data recovery, including those that may result from the negligence of computer forensics laboratory involved in the investigation. The customer will be expected to agree that he/she will not hold responsible any of the involved computer forensics laboratory for any direct or indirect damage or loss of equipment or media or data loss. In the case of any damage or loss to the original media or equipment, the liability of the forensics laboratory shall be limited to providing the customer with similar media or equipment of comparable price or capacity.

The maximum aggregate liability of computer forensics laboratory to the customer whether in contract, tort or otherwise for any direct loss or damage including to tangible property suffered by the customer as a result of any default of computer forensics laboratory shall be limited in aggregate to the lesser of the stated sum or an amount equal to the sums paid by the customer under the contract during the preceding number of days stated in the contract (typically 30 days).

Any advice or recommendations given to the customer by the forensics laboratory or its employees or agents as to storage, application and use or preference of the equipments which is not confirmed in writing by the computer forensics laboratory is followed or acted upon entirely at the customer's own risk. Accordingly computer forensics laboratory shall not be liable for any such advice or recommendation which is not so confirmed. Although the computer forensics laboratory is to make every effort to preserve the integrity of any data or equipment related to the engagement, the customer has to agree not to hold the forensics laboratory responsible for any accidental damages to the data or equipment in its possession including but not limited to surface scratches, deformations and cracks.

1. **Customer's representation:** Customer needs to warrant the forensics laboratory that he/she is the owner of, and/or has the right to be in possession of, all equipment/data/media furnished to the laboratory and that collection, possession, processing and transfer of such equipment/data/media are in compliance with data protection laws to which customer is subject to.

2. **Legal aspects/the law side:** Both the parties need to agree that the agreement shall be governed by prevailing law in every particular way including formation and interpretation and shall be deemed to have been made in the country where the contract is signed.
3. **Data protection:** The computer forensics laboratory (engaged in the investigation) will hold the information that the customer has given verbally, electronically or in any submitted form for the purpose of the forensics investigation to be carried out as per contracted services from the forensics laboratory. Customer may apply for a copy of the information that the laboratory hold about customer and customer has the right to have any inaccuracies corrected.
4. **Waiver/breach of contract:** The waiver by either party of a breach or default of any of the provisions on this agreement by either party shall not be construed as a waiver of any succeeding breach of the same or other provisions, nor shall any delay or omission on the part of either party to exercise or avail itself of any right, power or privilege that it has, or may have hereunder operates as a waiver of any breach or default by either party.

7.10.2 Solving a Computer Forensics Case

A real-life example, showing how a case is solved using forensics, is available in Section 11.6.2 (Digital Forensics Case Illustration 2: Analysis of Seized Floppy – the Drug Peddler Case). As for this chapter, we summarized this section by presenting the steps involved in solving a computer forensics case. These are just some broad illustrative steps and they may vary depending on the specific case in hand.

1. Prepare for the forensics examination.
2. Talk to key people to find out what you are looking for and what the circumstances surrounding the case are.
3. If you are convinced that the case has a sound foundation, start assembling your tools to collect the data in question. Identify the target media.
4. Collect the data from the target media. You will be creating an exact duplicate image of the device in question. To do this, you will need to use an imaging software application like the commercial *EnCase* or the open-source *Sleuth Kit/Autopsy*.^[9]
5. To extract the contents of the computer in question, connect the computer you are investigating to a portable hard drive or other storage media and then boot the computer under investigation according to the directions for the software you are using. It is imperative that you follow the directions precisely because this is where the “chain of custody” starts (refer to Section 7.8, Figs. 7.10 and 7.11, and Boxes 7.4 and 7.12). Make sure that you use a write-blocking tool when imaging the media under investigation. This makes sure that nothing is added to the device when you are creating your image.
6. When collecting evidence, be sure to check E-Mail records as well. Quite often, these messages yield a great deal of information (see Section 7.6 for E-Mail forensics).
7. Examine the collected evidence on the image you have created. Document anything that you find and where you found it. There are tools available to help look into open files, encrypted files, and mapped drives and to even analyze network communications. You can look into both commercial products and open-source products.^[6]
8. Analyze the evidence you have collected by manually looking into the storage media and, if the target system has a Windows OS, check the registry. Be sure to look into Internet searches as well as E-Mail and pictures that are stored on the target computer. Many times, criminals will hide incriminating information in pictures and E-Mails through a process called *steganography* (see Section 7.12).
9. Report your findings back to your client. Be sure to provide a clear, concise report; this report may end up as evidence in a court case.

7.11 Setting up a Computer Forensics Laboratory: Understanding the Requirements

There are four broad types of requirements, namely, the physical space, the hardware equipment, the software tools and the forensics procedures to be followed to aid those involved in the cybercrime investigation. Figures 7.12 and 7.13 show how a typical laboratory looks.

First of all there is a physical facility in which the laboratory is set up. This is meant to be the home base for secure storage of evidentiary materials, for the analysis of captured data, for the operation of cloned systems, for the production of final evidence reports and for the physical premises where the forensics professional will perform most of their duties and work. Therefore, it should be designed as a secure storage facility that can also house an office, an operational laboratory and a production facility all rolled into one. The lab home should also have a separate interview facility or a small office/cabin where interviews and/or collaborative investigative procedures can be carried out without disturbing any ongoing technical or forensics work. This is because an investigating officer or attorney with an in-depth knowledge of the case may have queries that can be answered more effectively in collaboration with the forensics investigator. The forensics professionals generally perform specific analysis and/or search actions to find the answer to questions posed by the investigating officer or attorney.

Physical floor space requirement for a forensics laboratory varies depending on the size of the group that will occupy it. The bottom line is that the laboratory space should be in a secure location or contain appropriate measures that will stop unauthorized access to the premises. It should have an adjacent and secure walk-in lock-up vault that can keep intruders from gaining access to its contents as well as to protect the contents from fire/heat, smoke, water and electromagnetic emanations and should generally not be near radio equipment. Figure 7.14 shows cyberforensics equipments and Fig. 7.15 shows different types of connectors that are used with forensics tools.



Figure 7.12 | Cyberforensics laboratory – 1.



Figure 7.13 | Cyberforensics laboratory – 2.

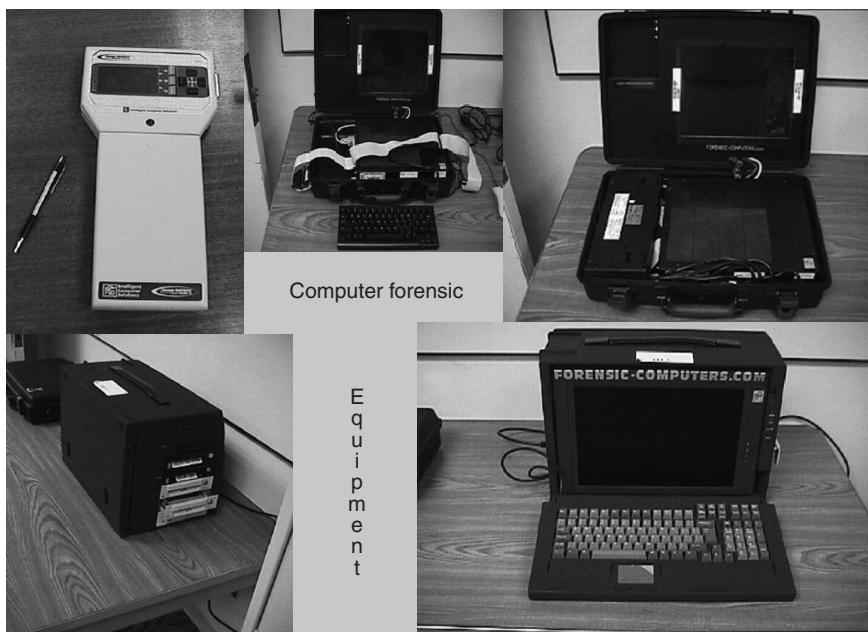


Figure 7.14 | Cyberforensics equipments.



Figure 7.15 | Connectors used with cyberforensics tools.

The laboratory stores valuable items from investigation perspective – seized equipment, as well as official certified evidentiary copies of seized data, will be stored in the fire-proof vault. With the appropriate enforced sign-out/in procedures, it will serve to maintain the chain of evidence (refer to Section 7.8, Figs. 7.10 and 7.11, and Boxes 7.4 and 7.12). Therefore, access to the vault and its contents should be logged as well as locked when not under use, and should be monitored at all times. There must also be adequate lockable storage space for various specialized equipments that will, over the course of investigations, be acquired and used for other investigation. This space must also accommodate consumables like CDs, DVDs, removable hard drives of various capacities, paper, toner cartridges, etc.



Apart from the physical space requirement, another key requirement for a computer forensics laboratory is the hardware items. The laboratory requires a number of computers, including a network server with a large storage capacity (preferably configured for the standard removable hard drives).

The server in the computer forensics laboratory is typically used to manage, document and administer cases, store various software tools and manage one-off specialist hardware. The hardware that must be managed includes, for example, devices like Rimage DVD Publishing Systems^[10] CD production units, CopyPro floppy disk readers, printers, etc. Figure 7.16 shows a disk duplicator equipment to give an idea about such hardware equipment required in a computer forensics laboratory.

The *evidentiary copy of seized data* is usually written to CD or DVD and, because of the large capacity of current hard drives, this can be a time-consuming process (see the paper quoted in References).^[11] Some disk duplication devices (the Rimage, and other units like it), make it possible to create, number and label the media unattended, producing as many as 50 CD/DVDs without intervention. Capturing the contents of floppy disks is even more time consuming, and devices like the CopyPro also can acquire as many as 50 floppy disks without intervention. The capabilities of these types of devices may vary from model to model; the two mentioned (Rimage and CopyPro) are merely examples with specific capacities. There should



Figure 7.16 | Disk duplication equipment in a forensics laboratory.

also be separate Internet connection(s) but NEVER connected to the forensics server. The Internet will be useful for finding and sharing forensics information and techniques and for communicating with other forensics professionals. Staying abreast of developments in this field is a vital part of staying current and updated in the forensics arena. The Internet provides one source to help accomplish this need.

The forensics laboratory also needs a number of workstations for connecting them to the internal network. The number of workstations required in the laboratory will depend on how many forensics expert staff members are employed to work in the laboratory. The workstations will enable them to work on individual cases simultaneously and have access to the shared devices and resources. Portable acquisition computers, that is, the *portable forensics kits* (Fig. 7.17) are also required as many times the forensics staff will need to work on the crime incident site. Ideally, each portable kit should be configured identically with the standard forensics suite of tools and removable hard drives (the same standard hard drives as mentioned earlier) of various capacities.

Each kit should have a robust carrying case that can accommodate extra hard drives. An array of associated connection plugs, converters and a hard drive write blockers (such as “FastBloc” for example) are available. An EnCase Accessory^[12] comes in two types – field edition and laboratory edition (Fig. 7.18). The field versions of the forensics kits will be used for onsite acquisition and/or seizure. It is usually preferable for acquisition to be undertaken in the controlled conditions of the laboratory; however, there are circumstances where this is not practical and an evidentiary acquisition must be undertaken onsite (e.g., when dealing with an Internet service provider).

These kits must also have an assortment of forms, such as labels, tags, pens, tape, evidence bags, an electronic camera, a GPSS, etc., all of which are vital to the process of seizure and acquisition. There will



Figure 7.17 | Portable forensics kits.



Figure 7.18 | FastBloc – the Field Kit and the Lab Kit. (a) The lab edition and (b) the field edition.
Source: Guidance Software's Product Catalogue/Data Sheet titled "The Next Generation of write blockers" can be accessed at the following link: http://www.forensics.ie/images/products/guidance_fastbloc_datasheet.pdf (8 January 2010).

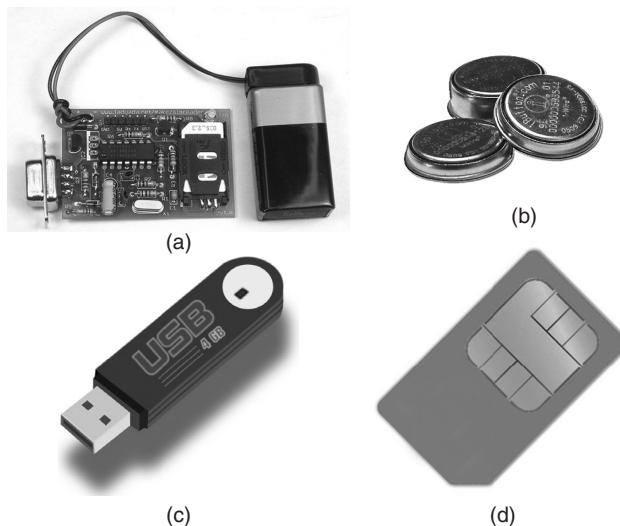


Figure 7.19 | (a) SIM card reader, (b) iButtons, (c) flash memory, (d) SIM card.

be an ongoing need to obtain devices, media, cables, converters and specialized media readers of various types, both for experimental purposes and for the acquisition of evidence from media other than hard drives or floppies (e.g., SIMs, flash memory of various description, iButtons, etc. – see Fig. 7.19). The hardware and physical premises constitute the largest outlay of funds. This, however, is an ongoing process and funds must be allocated regularly for the purchase of new hardware as it finds its way into the public arena.



On the software side, there are several requirements for setting up a forensics laboratory. The standard forensics software package, such as EnCase, WebCase, Forensics Tool Kit, Password Recovery Tool Kit, etc. are expensive products.

Some forensics kits require physical dongles to work and that these must be managed. A dongle is a physical security device (generally connected on the parallel port of the computer) that allows software to be used only when the device is present. In most cases, the capabilities of the software tool outweigh the nuisance and inconvenience of the required dongle. These products tend to be upgraded annually and, in each case, funds must be allocated for the upgrades. However, the software tools that are used comprise a far wider range than just those cited above. Many are freeware and many are not. No single tool performs the entire job of forensics acquisition, analysis and reporting; therefore, we need to use the right tool for the right task. Therefore, the forensics software tool library is extensive and it continues to grow. Having the right tool may make the difference between capturing relevant evidence and not being able to do so – as a result a case may be won or lost. In addition, the standard operational software will be required too; typically, this includes LAN software, OS, administrative software, graphics software, etc. These tools need to be upgraded occasionally; therefore, funds must be allocated for this ongoing process too. The continued cost of software acquisition and upgrades is usually smaller than that of hardware; however, it still constitutes a significant

portion of any forensics laboratory budget and must not be overlooked. The physical price of operating a forensics laboratory is not insignificant.

Orientation/mindset for procedure-based working is very important for a person working in a cyberforensics/computer forensics laboratory. One has to be very meticulous and should have a mindset for attention to details. This is important to be successful in digital forensics work like any other forensics work. Methods and procedures are an important part of operating a successful forensics laboratory.



The main issues that are attacked when evidence is presented in a court of law are credentials and methodology. In some countries, the court may prefer the forensics evidence from government appointed and/or neutral party laboratories rather than the evidence from private agencies where opportunities for manipulation/exploitation are perceived.

Close attention must be paid to strictly following and documenting the methodology adopted by the laboratory for the acquisition, analysis and reporting processes. Moreover, it is equally important to have a formal procedure in handling documents and control of evidence to be able to document the “chain of evidence.” These are the main aspects that are unique to a forensics laboratory. There are other procedures and policies that should be in place and enforced, but they are the standards like Internet usage, E-Mail rules, back-up methods, etc. (See Appendix C in CD.)

7.12 Computer Forensics and Steganography

Steganography is the art of information hiding. The threat raised by steganography is very real. Its use is not easy to detect or intercept, as the information does not need to be broadcast across the Internet. The hidden message can reside unsuspectingly on a website, for example, and can be viewed from around the world. The technology is undoubtedly being used for other immoral purposes.



“Steganalysis” is of increasing importance to cybersecurity. Hiding messages in image data, called steganography, is used by criminals and by noncriminals as well to send information over the Internet. The term “steganography” originates from the Greek term for “covered writing.”

Steganography was primarily used for “secret communications” to conceal the very existence of the message. Steganography is the art of “hiding information” in seemingly innocuous carriers in an effort to conceal the existence of the embedded information. Interestingly, steganography is not only the art of information hiding, but also the art and science of hiding the fact that communication is even taking place. Although “cryptography” is considered the predecessor of “steganography,” steganography differs from cryptography. Cryptography is the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the very existence of the secret communication. While steganography is separate and distinct from cryptography, there are many analogies between the two and, in fact, steganography is categorized as a form of cryptography since *hidden* communication certainly is a form of *secret* writing. In a way, “steganography” and “cryptology” are guided by the same motive that is, to make a message useless for those who want to read it. When steganographic techniques are used, the *message cannot be seen* because it

is hidden and with cryptology techniques applied the *message cannot be deciphered* although it is not hidden. There is one distinct difference, cryptography is dependent on hiding the meaning of the message, whereas steganography is dependent on hiding the presence of a message altogether. Steganography accomplishes its objective through exploiting the Internet technology. The sheer size of the Internet and its vast amounts of data are what accomplishes this fete, and for this reason, it can be a very effective method of securing data transfer, which most of the time is used by the cybercriminals.

Steganography, by its very nature, poses a threat to forensics analysts, as they now must consider a much broader scope of information for analysis and investigation. Steganography is, therefore, considered as one of the “antiforensics methods.” “Computer antiforensics” are methods of removal and subversion of evidence with the objective to mitigate results of computer forensics. There are other methods too that act as computer antiforensics, namely, encryption, self-splitting files plus encryption, database rootkits, BIOS rootkits, bypassing integrity checkers, etc. Let us understand “rootkits.”

Box 7.13 Steganography, Cryptography and Digital Watermarks

It has been a long-standing desire of human beings to keep sensitive communications secret. Guillermito classification of steganographic software^[13] mentions that the following is possible:

1. Adding data at the end of the carrier file;
2. inserting data in some junk or comment filed in the header of the file structure;
3. embedding data in the carrier byte stream, in a linear, sequential and fixed way;
4. embedding data in the carrier byte stream, in a pseudorandom way depending on a password;
5. embedding data in the carrier byte stream, in a pseudorandom way depending on a password, and changing other bits of the carrier file to compensate for the modifications induced by the hidden data to avoid modifying statistical properties of the carrier file.

As mentioned before, “Steganography” is the art of covered or hidden writing. The purpose of steganography is “covert communication” to hide a message from a third party. However, this is different from “cryptography,” that is the art of “secret writing,” which is intended to render a message unreadable by a third party. However, cryptography does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many similarities between the two; therefore, some people categorize steganography as a form of cryptography, as hidden communication is a form of secret writing.

Now let us understand the difference between encryption and steganography. Contents of information kept private and confidential using “encryption” so that only those who have the proper keys (privacy key and public key) can extract the secret contents. On the other hand, the sole purpose of using steganography is to hide the fact of secret message (possibly containing the evidence) if it exists. Therefore, the military calls this “covert communication” and the path for this kind of communication is called “covert channel.”^[14] Some good reference links on “covert channels” are provided in Ref. #10, Additional Useful Web References and in Refs. #14, #15 and #20, Articles and Research Papers, Further Reading.

Note yet another difference: steganography hides the covert message but not the fact that two parties are in communication. Steganography techniques generally involve placing a hidden message in some transport medium called the “carrier.”

“Digital Watermarking”^[15] is conceptually similar to steganography; however, its technical goals are different. Generally, only a small amount of repetitive information is inserted into the carrier and it is not necessary to hide the watermarking information. It is useful for the watermark to be able to be removed while maintaining the integrity of the carrier. Refer to Appendix N in CD.

Cryptography is discussed in Ref. #16, Books, Further Reading.

7.12.1 Rootkits

The term rootkit is used to describe the mechanisms and techniques whereby malware including viruses, Spyware and Trojans attempt to hide their presence from Spyware blockers, antivirus and system management utilities. Rootkits can be classified as – persistent rootkits, memory-based rootkits, user-mode rootkits and kernel-mode rootkits. These classifications are made depending on whether the malware survives reboot and whether it executes in user mode or kernel mode. Basically, a “rootkit” is a set of tools used after cracking a computer operating system that hides logins, processes, password, etc., which would carefully hide any trace that those commands normally display. Rootkits are installed after an attacker has exploited a system vulnerability and gained root access. Rootkits by themselves do not give an attacker root access; they only work after a system compromise. Rootkits consist of tools that generally have three functions: (a) maintain root access to the system, (b) hide the presence of the attacker and (c) attack (or accelerate attacks) against other systems. From attacker’s perspective, rootkits serve following important functions:

1. The first, and primary, function of a rootkit is to maintain access to the compromised system. This access can happen via any communication channel from an easily detectable telnet shell to a secure shell to covert communication channels overlaid over commonly used protocols. An attacker who cannot maintain access to a host cannot exert his or her control over it.
2. The second main function of a rootkit is to hide, or otherwise obfuscate, the presence of the attacker. The ability to hide the presence of an attacker is what makes the rootkit such a powerful tool and is critical to the success of an attacker in maintaining root access to a system. This is achieved by removing evidence of the compromise and taking measures to misrepresent the system state to curious or confused system administrators. Removing evidence can be achieved through cleaning various log files and temporarily disabling any monitoring demons. How a rootkit chooses to hide its presence and the presence of the attacker is the qualifying characteristic of the rootkit. For example, an attacker could replace commonly used system executables, re-route system calls and install a loadable kernel module in a single rootkit installation. Attackers typically choose more than one method of hiding their presence (like for “defense in depth” think “offense in depth”!).
3. The third function of a rootkit is to perform actions that meet the attacker’s objectives, mainly by attacking or aiding in attacking other systems. This usually means compromising host security (e.g., by using keyloggers), gathering packet traces on the local network, performing vulnerability scans or even launching automated attacks from the compromised host.

Now let us understand “binary rootkits.”

Binary rootkits take administrative utilities and modify them to hide specific connections, processes and activities of specific users. These utilities would also include tools to provide root access to a particular user or when supplied with a particular argument. For example, an attacker could modify the “w” binary to hide his/her user account while logged on, the “ps” command to hide any processes he/she is running, and the “su” command to always allow root access whenever a specific password is supplied. These changes are not limited to the binary files only but source files can also be directly modified by attackers. If the source code is not examined for these inconsistencies, a rebuilt binary that is assumed to be “clean” can be compromised. When the binary tools are deployed, they are often placed inside of a hidden directory until the administrative programs can be fully compromised. An aspect of social engineering is used when creating these directories. Some of the common locations include confusing or unsuspecting directory names, such as /dev/.hdd or /dev/.lib. Others include commonly overlooked directory names such as /etc/... or /etc/”.. “ (dot-dot-space). There are, of course, defenses available for rootkits. Let us take a brief look at them.

Binary rootkits can be defeated through the use of file integrity scanners. Most file integrity scanners work by computing checksums, cryptographic checksums or even digital signatures. The file signatures must be created when the system is in an uncorrupted state and are useless if not prepared before a rootkit has been installed. The cryptographic checksum itself is not immune to attack, and care should be taken that it is not recomputed with the corrupted media and overwritten (by writing them to immutable media and storing them offline, for example). However, successful use of this technique also means that any legitimate patches or updates must be followed up by recomputing the checksum (a technique that may fail in practice for frequently updated systems). Binary rootkits can also be detected by system integrity tools. However, certain commonly changed or temporary directories may be ignored by the system integrity scans, so care should be taken by the system administrator to inspect these directories for unusual activities. Further discussion of each of these methods is beyond the scope of this chapter. Readers interested in greater details of these topics should refer to Ref. #4, Additional Useful Web References, Further Reading and Ref. #4, Video Clips, Further Reading.

7.12.2 Information Hiding

Let us now have an overview of some characteristics of information hiding and then we discuss about steganalysis methods for determining the existence of and potential locations of hidden information. Today we are in the “digital age” where the messages can be hidden in images, sound files, text and other digital objects. These messages are invisible to a casual observer. The use of “steganography” on public networks, such as the Internet, is unknown due to its stealthy nature. Unless it is being actively looked for, one would not know that it is there. For example, pop-up ads, photos on sales and purchase portals such as eBay, and

Box 7.14 Hair Splitting Experience for Forensics Investigation Experts!

“Self-splitting files” is a method developed by the Intruders Tiger Team Security. The technique consists of the following:

1. A framework that interprets input files (binary or texts) and places them in sectors marked as bad blocks (but in the truth, they are not).
2. An input file (binary or text) that is divided in several asymmetric parts that are encrypted and placed outside of order in bad blocks;
3. An input file (binary or text) that is wiped after having been processed.
4. An input file (binary or text) that can be in a HTTP(s) or FTP server, and is processed without touching the disk (all in memory).
5. A library that allows the easy interaction of framework with sniffers, etc.
6. A tool that returns a sequence of blocks and a pseudorandom key that must be known to read, remount or execute the file.

Another technique used is the Wipe utility; it makes things difficult for the cyberforensics experts and investigators. Wipe is a name given to the method of safe deletion. In the current file systems, the files are not totally extinguished. When we delete a file (with “rm,” “del,” etc.), the field “link count” is set to zero and the field “deleted time” to the hour that the file is excluded. Therefore, the files can be easily recovered via software methods used in computer forensics. A method to make the recovery of files difficult is the use of the Wipe that does nothing more than open the file and overwrite it several times with pseudorandom (or predefined) content and later unlinks them from “inode” and “directory entries.”

Examples of utility are necrofile e klismafile (the Defiler’s Toolkit). Even after Wipe’s method, files can be recovered through a “ferromagnetic” phenomenon that is called “hysteresis loop.” However, this type of computer forensics method requires equipment with highest cost, and the recover process being each day more and more complex because of the increase of hard disk density and the number of overwrites made by the Wipe.

other recreational sites, all have the potential of containing hidden messages. An average organization is not expected to take on the vast responsibility of searching large websites and newsgroup areas for potential steganographic images. Most organizations can and do, however, monitor network traffic that is entering and exiting the local area network.

The first question is why one would want to “hide” information. In the first category, there are those who are trying to protect their intellectual property rights. There is a high availability of information via the Internet and that makes it increasingly difficult to protect intellectual property and enforce copyright laws. The use of “digital watermarks”^[15] provides a way to insert a copyright notice into a document or image. The watermark is often a small image or text that is repeated frequently throughout the document or image. A similar technique is to embed a digital fingerprint or serial number. Fingerprint presents a certain advantage in that it can be used to trace the copy back to the original and thus it is a powerful tool for prosecuting copyright violators. Therefore, this is about the first category of people who would be interested in “hiding” information.

In the second category are people who are interested in hiding information to convey information in a covert manner and avoid observation by unintended recipients. In this case, the hidden message is more significant than the “carrier” object that is used to transport it. Steganography is often compared to cryptography in its ability to restrict unauthorized access to information. Cryptography is used to encrypt or scramble the data in such a fashion that only the intended recipient can decrypt it. At the outset of this discussion, we explained the difference between “cryptography” and “steganography.” There are three common approaches of hiding information in digital images^[16] (a) least significant bit insertion, (b) masking and filtering and (c) algorithms and transformations.

Box 7.15 Hide and Seek in the World of Information Communication

An interesting question is “how do we hide information in the electronic age?” Computers use binary, a combination of zeros and ones to represent text and graphics. The ASCII (American National Standard Code for Information Interchange) is the de facto standard for representing text and certain control characters. ASCII uses one parity bit and seven data bits to represent each character in the English language. For example, an uppercase “A” is represented by 1000001. A digital image is composed of picture elements or “pixels.” Each pixel contains information as to the intensity of the three primary colors: red, green and blue. This information can be stored in a single byte (8 bits) or in three bytes (24 bits). For example, in an 8-bit image white is represented by the binary value of 11111111 and black by 00000000.

Current information hiding techniques rely on the use of a cover object (image, document, sound file, etc.) – sometimes known as a carrier. The secret message is then broken down to its individual bits by a steganographic tool (stego-tool) and embedded in the cover object. Many tools will utilize a password or pass-phrase that is necessary to extract the hidden message and is referred to as a stego-key. The result of this process is known as the stego-object.

One would wonder where can information be hidden. Almost anywhere on the Internet! The standard protocol suite used on the Internet is the Transmission Control Protocol/Internet Protocol (TCP/IP). The headers used to transfer data between computers allow the use of flags and certain reserved fields. With the appropriate tool, information can be inserted into these fields. The advantage of this technique is that headers are rarely read by humans and thus makes an ideal place to hide data. The disadvantage of this method is that firewalls can be configured to filter out packets that contain inappropriate data in the reserved fields, thus defeating the steganographic transmission.

Another popular technique for hiding information is to include extra spaces in documents. These spaces may contain hidden characters. Again this is a simple technique for hiding information and consequently is easy to detect and defeat. By opening such a document in a word processor the unusual spacing becomes readily apparent. Reformatting the document can remove the hidden message. The use of audio files can provide a good carrier for hidden messages. By their very nature, sound files tend to be large in size and thus do not attract attention. In particular, the MP3Stego tool can be used to hide information and maintain nearly CD quality sound.

Criminals do a number of activities with their data – they delete data, destroy data, hide data or may also encrypt data – all with the purpose that the traces of their criminal deeds do not fall in the hands of the investigator. As for data destruction, “data sanitization” is an important term to understand. By definition, ‘sanitization method’ is the specific way of using a data destruction program to overwrite the data on a hard drive or other storage device. Technically speaking, there are other methods as well for destroying data. These methods are not based on software overwriting and are also referred to as “data sanitization methods.” Often a question is asked as to which method for data sanitization is the best one. An often quoted method in this regard is the *DoD Data Sanitization Method* – for example the DoD 5220.22-M data sanitization method is usually implemented as a ‘3-pass method’:

1. In Pass 1: “0” is written and the write is verified.
2. In Pass 2: “1” is written and the write is verified.
3. In Pass 3: a random character is written and the write is verified.

There seems almost a universal agreement that overwriting an entire hard drive once with a single character prevents recovery of data from a hard drive even if any software based file recovery method is used. It is believed that most data sanitization methods are over-kill. They claim that a single overwriting of data is adequate to prevent data recovery even if advanced; hardware-based methods are used for extracting information from hard drives. There, however, does not seem to be a universal agreement about this.

We conclude this discussion on the note that there are concerns that terrorists are using steganographic techniques for hiding their messages, terror-related events inside images, text that is displayed on the Internet sites. As the research in steganographic method advances, there can be hopes of abetting the secretive communication methods used by the terrorists in propagating their illicit messages on the Internet about their destructive work. To conclude steganography is one of the threats that needs to be considered and understood for possible future occurrences.

7.13 Relevance of the OSI 7 Layer Model to Computer Forensics

The OSI 7 Layer Model is useful from computer forensics perspective because it addresses the network protocols and network communication processes. The basic familiarity with the OSI 7 Layer Model is assumed for the discussion in this section. To know more about OSI Model and network protocols, refer to Ref. #15, Books, Further Reading. The OSI Model depicted in Fig. 7.20 shows Internet Protocols involved at each of the seven layers. Forensic analyst needs to very well understand how the TCP/IP works.^[17] To effectively perform forensics network analysis, forensics professionals must have a strong understanding of underlying network processes and protocols. Explaining these concepts is beyond the scope of this chapter. Interested readers may refer to the relevant chapter mentioned in Ref. # 15, Books, Further Reading.

In Chapter 1, it was mentioned that “hacking” is one of the cybercrimes – it involves unauthorized access to a computer system. Effective penetration testing requires complete understanding of the methods and motivations of a typical hacker. The steps taken by attackers who hack networks are shown in Fig. 7.21; each is briefly described.

7.13.1 Step 1: Foot Printing

Foot printing includes a combination of tools and techniques used to create a full profile of the organization’s security posture. These include its domain names, IP addresses and network blocks. Some of the tools used

		OSI layers			Protocols, browser, Calls and browser-based languages			
			NFS	Web browser	E-Mail client	Windows file and print sharing		
		Ping (command)	XDR	HTML	MIME			
		Session	RPC	HTTP	SMTP			
Layer 7		Application					RPC and SMB	
Layer 6		Presentation						
Layer 5		Session					NetBEUI	
Layer 4		Transport	ICMP	UDP	TCP			
Layer 3		Network	IP				802.2	
Layer 2		Datalink						
Layer 1		Physical	Ethernet				Ethernet	

Figure 7.20 The OSI 7 Layer Model with Internet Protocols. Abbreviations: UDP, User Datagram Protocol; IP, Internet Protocol; ICMP, Internet Control Message Protocol; TCP/IP, Transmission Control Protocol/Internet Protocol; RPC, remote procedure calls; HTTP, Hypertext Transfer Protocol; SMTP, Simple Mail Transfer Protocol; XDR, eXternal data representation; HTML, hypertext markup language; MIME, multipurpose Internet mail extensions; SMB, server message block; NFS, network file system.

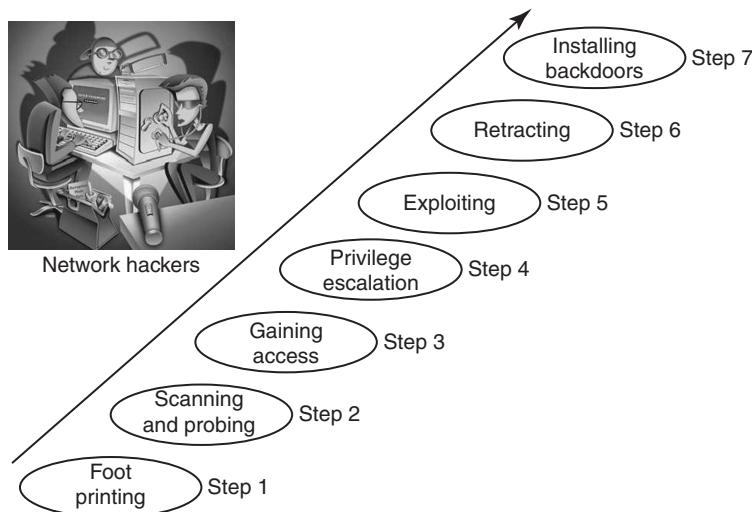


Figure 7.21 Network hacking steps.
Note: This is being illustrated how hacking takes place.

for footprinting are SamSpade, nslookup, traceroute and nettrace (refer to Tables 2.1 and 2.2 in Chapter 2 for a list of tools used during the “active attack” phase). Once the IP address and domain names are known, a hacker will typically perform a series of scans or probes to gather more information about individual machines for the purpose of gaining unauthorized access to the system at a later date. These scans may include ping sweeps, TCP/UDP scans and OS identification. All of these actions can be performed with a single tool called Nmap. Nmap is a free security scanner written by Fyodor.

The tool called “Metasploit” (mentioned in Table 4.1, Chapter 4) was developed as an automated tool to provide useful information to people who perform penetration testing. To know more on penetration testing, refer to Ref. #19, Books, Further Reading. In addition to providing this service, it has also become an automated tool to gain access to insecure computer systems. Metasploit groups exploit both OS and application. Performing a successful exploit has now become as simple as finding out the target’s OS or application, entering the target’s IP address and pressing a button.

7.13.2 Step 2: Scanning and Probing

The hacker will typically send a ping echo request packet to a series of target IP addresses. As a result of this exploratory move by the hacker, the machines assigned to one of these IP address will send out echo response thereby confirming that there is a live machine associated with that address. Similarly, a TCP scan sends a TCP synchronization request to a series of ports and to the machines that provide the associated service to respond. Finally, using tools such as Nmap, the hackers can determine device type and OS details by interpreting the responses. System scanning and probing can provide insights about the easiest path into the targeted system to a hacker. Gaining access takes advantage of specific security weaknesses in the system to allow access via an individual machine.

Uneducated hackers were known as “script kiddies” (refer to Chapter 10) because they could gain access to target machines via scripts that were published on hacker websites. These hackers are increasingly known as “click kiddies” because the process has become as easy as clicking a button. Figure 7.22 shows the network hacker categories.

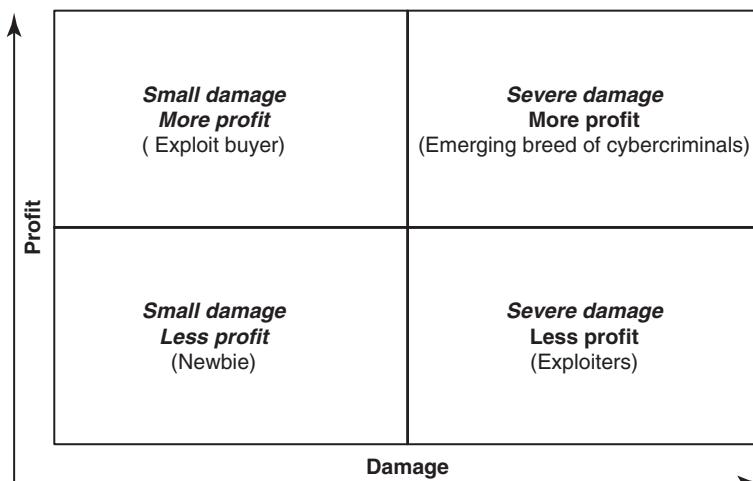


Figure 7.22 | Hacker categories (profit and damage).

7.13.3 Step 3: Gaining Access

The hacker's ultimate goal is to gain access to your system so that he/she can perform some malicious action, such as stealing credit card information, downloading confidential files or manipulating critical data. As each device and OS in your network has a unique security posture, the information provided during system scanning and probing can give the hacker insight as the easiest path into your system. Gaining access takes advantage of specific security weaknesses in the system to allow access via an individual machine.

7.13.4 Step 4: Privilege

When a hacker gains access to the system, he will only have the privileges granted to the user or account that is running the process that has been exploited. Gaining access to root or administrator will allow the hacker more access or greater power throughout the network. All hackers, therefore, would like to gain root or administrator privileges on the network. An exploited application that is running under a root user will give the hacker immediate root access. However, if the application that is exploited is not running under a root, the hacker must perform additional actions to earn it. This usually entails trying to crack the passwords.

7.13.5 Step 5: Exploit

Gaining root access gives the hacker full control on the network. Every hacker seems to have his/her own reasons for hacking. Some hackers do it for fun or a challenge, some do it for financial gain and others do it to "get even" (see Fig. 7.21). Exploiting the system, therefore, will take many forms. Hackers who do it for fun or a challenge will generally change a webpage or leave a "calling card" to let his peers know that he/she was successful. Hackers fall into this category. More often, hackers try to break into systems for financial rewards. This will generally help them to download valuable information that can later be sold to other parties. Sometimes, there can be a disgruntled employee who may gain access to sabotage an important project.

7.13.6 Step 6: Retracting

There are many reasons (as mentioned in Section 7.13.5) that drive cybercriminals to hacking. Whatever the motive, hackers do not want to be caught and sent to jail. Therefore, the next step in the hacker methodology is covering tracks. The hacker will usually take the time and effort to modify system logs to hide his/her actions and try to mislead forensics investigators that a crime has been committed. Refer to Table D.II.13 in Appendix D (in CD).

7.13.7 Step 7: Installing Backdoors

Finally, most hackers will try creating provisions for entry into the network/hacked system for later use. This, they will do by installing a backdoor (see Chapter 4) to allow them access in the future. A backdoor is a security hole deliberately left in place to allow access from an uncommon/unobvious path. These can usually be easily detected by skilled security professionals. In fact, almost all of the actions performed by a hacker can be detected by a forensics investigator. They just need to know where to look.

Professional working in the domains data networking and security would understand the terms "Layer 3" or "Layer 2" or "Application Layer." This terminology stems directly from the ISO Model and how it is applied to practical solutions. The model concepts are conventionally used to design and troubleshoot networks, and the 7 Layer Model is the standard for designing the network protocols. Careful study of the OSI 7 Layer Model can show us support for concepts that we have learnt from more conventional forms

of information security theory. Understanding and applying the model to information security scenarios can also help us assess and address information security threats in a network environment, allowing us to organize efforts to make security assessments and perform forensics analysis of compromised systems and threats presented in theory and found operating in the wild.

Cyberforensics experts have the technical skills that are useful for reading “obfuscated IP addresses.” Those who send Spam, unsolicited commercial junk mail, usually try to keep their true identities secret – otherwise, they would take the brunt from the disgruntled Internet citizens who wish to retaliate. In addition to using a bogus return E-Mail address, they often include obfuscated URLs. Instead of having a human-readable name, or the dotted-decimal format such as 135.17.243.191, a URL may appear in 10-digit integer format (base 256), so it appears like this: <http://2280853951>. More details like this to illustrate the technical skills in cyberforensics investigation are addressed in Chapter 11.

7.14 Forensics and Social Networking Sites: The Security/Privacy Threats

Social networking is one of the most popular activities across the globe in today's digitally connected networked world. Orkut, Facebook, MySpace, Bebo, “Bigadda” (an Indian social networking site), etc. are some familiar names of social networking sites. They are not the only ones, however. There are a surprisingly large number of social networking sites.^[18] Technically speaking, a “social networking site” is defined as Web-based services that allow individuals to:

1. Construct a public or semi-public profile within a bounded system;
2. articulate a list of other users with whom they share a connection;
3. view and traverse their list of connections and those made by others within the system; the nature and nomenclature of these connections may vary from site to site.

Using a social networking site brings like-minded people together for chat, conversation, exchanging ideas and even meeting in real life. Social networking is a popular activity in the Internet days because, it enables people to reach out to their old/long lost friends and classmates, relatives, etc. who may have migrated to other countries. Social networking sites even help connect like-minded people, people with the same professions or collaboration and discussion of ideas. Social networking, thus, makes people part of a worldwide community and so the sites are getting popular. Social networking has thus, become an extension of “sitting around the camp fire” and discussing life events. It is, then, no wonder that the usage of social network sites has increased rapidly in recent years.

Kids, teenagers are the ones who are known to be making the maximum use of social networking sites. There are professional networking sites too; for example, the most famous “LinkedIn.” LinkedIn is a social networking website oriented toward professional networking with over 10 million users spanning 150 industries and more than 400 economic regions. Users are able to and encouraged to create a profile including such information as resumes, job offers and past employers and then to build up a list of connections. The user profile and list of connections can help to gain introduction to someone the user wishes to know through a mutual contact, to find jobs and business opportunities, search for potential candidates (if the user is an employer), etc. While this may be so, there is a lot of discussion these days about the security threats through careless use of social networking sites. Almost everyday, there is some news or other about how people (especially the young generation) are victimized as a result of indiscrete use of social networking sites.

Current litigations, regarding social networking sites, have raised a number concerns: (a) whether the content social networking site violate people's intellectual property rights, (b) whether social networking sites

infringe the privacy of their own users or (c) whether fraudulent or other illegal activity, such as the sale of “knock-off” luxury goods or the promotion of prostitution, occurs with actual or collaborative knowledge shared in the social networking media community. Although these concerns may be perceived by some people as mere exaggerations or over-reaction to the rise of social media networking, the fact remains that adequately preserving the content at issue is critical. Content preservation can be challenging given the dynamic, short-lived and often multi-format nature of social media. In order to properly collect and authenticate social networking content, there is indeed a need for using tools and for executing emerging forensics methodologies. Like in other forensics circumstances, here too, it becomes essential to maintain robust chain of custody documentation to ensure that this highly relevant evidence is authenticated for admissibility. There is generally no control over the content posted on social media networking sites. Even if forensics data has been preserved, high level of forensics skill is required to analyze and quantify the preserved data to answer questions such as:

1. Who posted the offending content?
2. Is there a ‘real live’ person to whom the offending content can be attributed even when evidence exists?
3. Can we identify the time frame associated with the posting of the offending content?
4. How much of the offending content exists across the entire social networking platform?
5. Is there other evidence that corroborates or supports interpretation of the relevant content?
6. How accurate is the reported physical location?

Such forensics analysis of social media websites/social media networking sites is the need of the hour given criminal activities abound.



Criminal activities can arise from the use of social network sites.

For example, a mother was convicted of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed suicide.^[19] There seems to be no respect for “privacy” as if it has become a thing of the past. For example, although LinkedIn is generally well perceived by the media, there seem to be two main privacy issues: (a) LinkedIn does not allow you to remove your profile and (b) it shows member profiles. The good news is that the first privacy concern is now addressed in LinkedIn’s privacy policy. The second privacy concern is, surprisingly, perceived as one of the good things about LinkedIn.

All is not well even with “better of kind” professional networking sites like LinkedIn. For example, according to some people LinkedIn first builds the trust of the user, then hooks the user into the system by using easy-to-use simplified forms and finally gets the user to invest through the use of nagging tools.

Facebook (www.facebook.com) is one of the biggest online social networking websites, hosting approximately 25 million users. The website was originally created in February 2004 for college and university students, but since September 2006, it has become available to anyone with an E-Mail address. Facebook has many enticing features that allow users to join many networks (including university networks, geographic networks, vocation networks, etc.), to join groups of common interest and to upload pictures. Figures 7.23 and 7.24 show some interesting data about privacy concerns with regard to social networking sites and the age distribution of social networking site users.

The success of a social networking site depends on the number of users it attracts. In the attempt of wooing the users to their sites and thereby generating revenues, the designers of social networking sites also incline toward making available some material on these sites which may not always be decent. Generally, the

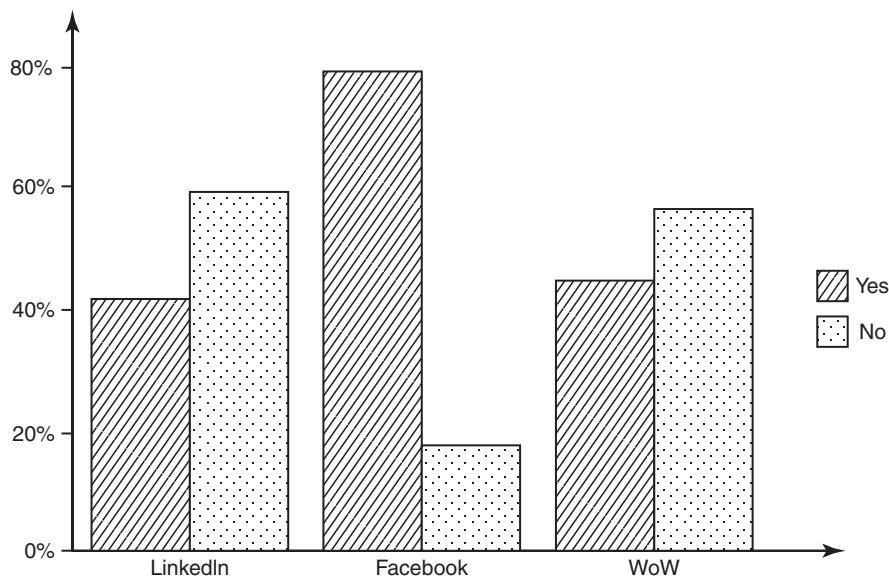


Figure 7.23 User concerns about privacy on social networking sites (LinkedIn, Facebook, WoW).

Source: The Paper by Helen Drislane and Kelly Heffner, 14 May 2007, is available at <http://www.eecs.harvard.edu/cs199r/fp/HelenKelly.pdf> (25 January 2010).

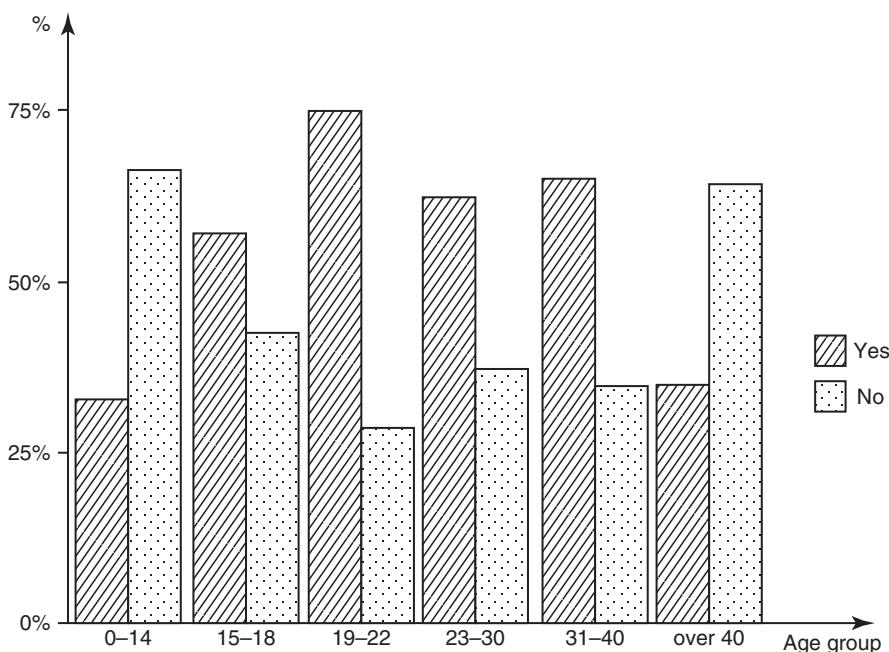


Figure 7.24 Privacy concerns about social networking sites vary with age.

Note: This is with regard to openness about sharing personal information.

Source: The paper by Helen Drislane and Kelly Heffner (14 May 2007) is available at <http://www.eecs.harvard.edu/cs199r/fp/HelenKelly.pdf> (25 January 2010).

aim of a social networking site is to design the site in such a way that encourages behavior to increase both the number of users and their connections. Unfortunately, like any fast growing technology, security has not been a high priority in the development of social network sites. Owing to this, that is, lack of security thinking in the design of social networking sites, significant risks have resulted. At times, these risks seem to outweigh the benefits obtained from the social networking websites.

There are privacy concerns that arise from the use of social networking sites. For example, Facebook's Beacon service tracks activities from all users in third-party partner sites, including people who never signed up with Facebook or who have deactivated their accounts. Beacon captures data details on what users do on the external partner sites and sends it back to Facebook server, along with users' IP addresses, the addresses of webpages the user visits, etc. This is an example of vulnerability in Facebook. Table 7.6 lists the security features on the top 10 social networking websites of 2009 and Table 7.7 shows security features for the top ten social security networks rated in the year 2010.



There are a number of security issues associated with social networking sites.

Security issues that are associated with social networking sites are listed below:

1. Corporate espionage.
2. Cross-site scripting.
3. Viruses and worms.
4. Social networking site aggregators.
5. Spear Phishing and social networking specific Phishing.
6. Infiltration of networks leading to data leakage.
7. ID theft (Phishing and Identity Theft is discussed in Chapter 5).

Table 7.6 | Top 10 social networking sites (year 2009) – security features

Social Networking Site Name	Supports HTML?	Does the Site Track Visitors?	Does the Site have Customizable Privacy Settings?
Facebook	No	No	Yes
Orkut	No	Yes	Yes
MySpace	Yes	No	Yes
Bebo	No	No	Yes
Friendster	No	Yes	Yes
Hi5	Yes	Yes	Yes
Netlog	No	No	Yes
PerfSpot	Yes	Yes	Yes
Yahoo!360	Yes	No	Yes
Zorpia	No	No	Yes

Note: The listing in Table 7.6 is not in the order of 2009 rating for the sites. It is in the order of "familiarity" of the site name assuming general public familiarity with those names of the sites. In year 2009 "Bebo" had rating 1 while in Year 2010 "Facebook" has got Number 1 rating. In year 2009 "MySpace" had No. 5 rating while in year 2010, it was rated No. 2. "Friendster" enjoyed No. 3 rating in year 2009 whereas its rating in year 2010 has gone down to No. 4. (Source of these changes rating is the link mentioned at the bottom of Table 7.7).

Table 7.7 | Top 10 social networking sites (year 2010) – security features

<i>Site Name</i>	<i>Privacy Settings Available?</i>	<i>User Blocking Available?</i>	<i>Spam Reporting Available?</i>	<i>Abuse Reporting Available?</i>	<i>Safety Tips Available?</i>
Facebook	Yes	Yes	Yes	Yes	Yes
MySpace	Yes	Yes	Yes	Yes	Yes
Bebo	Yes	Yes	Yes	Yes	Yes
Friendster	Yes	Yes	Yes	Yes	No
Hi5	Yes	Yes	Yes	Yes	Yes
Orkut	Yes	Yes	Yes	Yes	Yes
PerfSpot	Yes	Yes	No	Yes	Yes
Yahoo!360	Yes	Yes	No	Yes	Yes
Zorpia	Yes	Yes	No	Yes	No
Netlog	Yes	Yes	Yes	Yes	No

Note: There is full features comparison available in addition to the security features mentioned in the table above. The site overall rating for the social networking sites is available at: <http://social-networking-websites-review.toptenreviews.com/> (24 January 2010). (Sites are listed in the order of year 2010 rating).

- 8. Bullying.
- 9. Digital dossier aggregation vulnerabilities, secondary data collection vulnerabilities, face recognition vulnerabilities.
- 10. Content-based image retrieval (CBIR).
- 11. Difficulty of complete account deletion.
- 12. Spam.
- 13. Stalking.

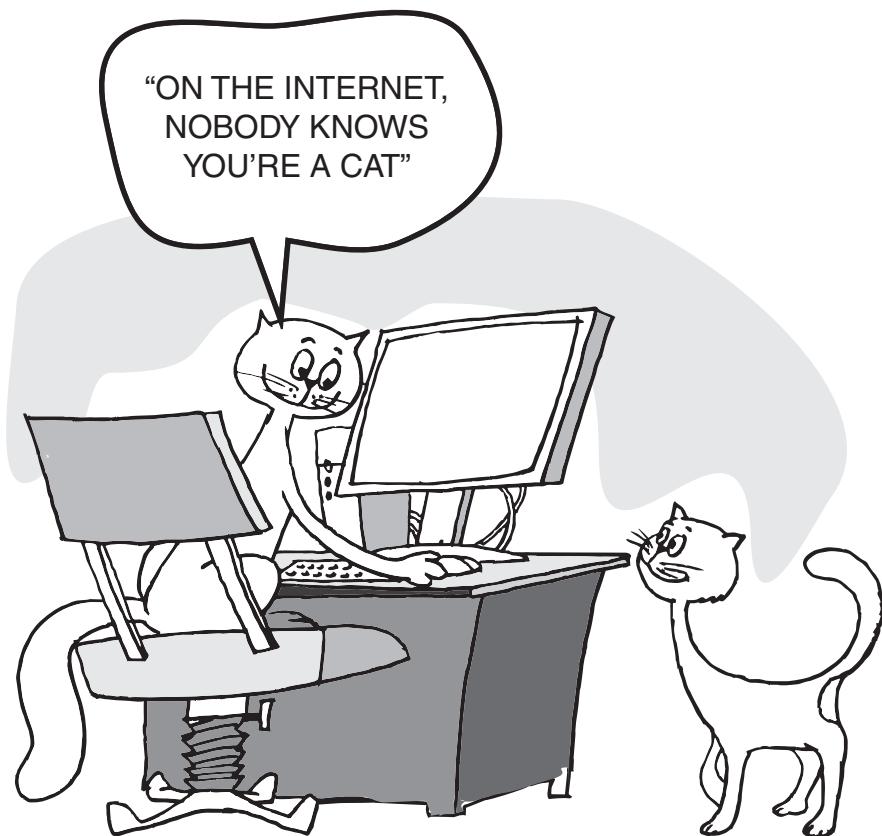
MySpace does not allow Java Script code to be used in their site. However, it does allow HTML code. MySpace and Hi5 allow their users to have the ability to add HTML code that can link to scripts and objects designed to retrieve other visiting user's information. The users of PerfSpot cannot add HTML code to their pages, but there are restrictions on the contents of this code. Yahoo!360 lacks detailed security controls as to who can view the user's profile. Their option is either everyone can view their blog or just friends. In other social networks such as Facebook and MySpace, specific security features are available to provide users with more control over their personal information. Friendster, Hi5, Orkut and PerfSpot users have the benefit of monitoring their profile visitors. This option increases awareness, protection and eases user tracking. Orkut is the only social network that forces the user's viewing history to be revealed if he/she decides to track other users who had viewed his/her profile.

It is possible to retrieve information about the users who visit your profile on social networking sites. Some of these sites provide built-in applications that show the usernames of the people who visit your profile. Other sites store log transcripts, which capture chat session information such as username and date. The function of user data retrieval can be accomplished within a website with user incorporation of either Java Script or Hypertext Preprocessor (PHP) code. Some social networking sites have restrictions in place to make Java Script and/or PHP code inactive when users try to incorporate into their site. There are different methods for capturing the non-personal identifiable information of users who communicate with each other in the virtual world. We have established that user data retrieval can be achieved with use of Web-based scripts.

User data can be retrieved and user data retrieval methods take place in the online environments of websites, IM chat sessions (virtual meetings) and E-Mails. From the user data retrieval methods used, the most important non-personal-identifiable user information that can be retrieved is the IP address. An IP address

Table 7.8 | Retrieving sender's IP address from E-Mail received

<i>Gmail</i>	<i>Hotmail</i>	<i>Yahoo mail</i>
<ol style="list-style-type: none"> 1. Access your inbox. 2. Select the message you would like to trace for its IP. 3. Click on the upside down triangle located on the right, next Reply. You will see options such as "Reply to all," "Forward," "Filter Messages like This," etc. 4. Select "Show Original." 	<ol style="list-style-type: none"> 1. Make sure you are in classic Mode. 2. Right click on the message. 3. Select "View Message Source." 	<ol style="list-style-type: none"> 1. Select the message. 2. Right click on the message. 3. Click on "View Full Headers."

**Figure 7.25** | On the Internet, it does not matter “who” you are as long as you have “ID”!!

can be used for tracking back to a user's location or the user's Internet service provider location. After retrieving the IP address, there are many links available for retrieving the geographical location of the user. It is possible to write a utility to track the visitors to a social networking site. The scripts for developing such utilities can work on any social networking website which allows you to embed HTML code in your homepage. The social networking sites and sales transaction websites that support visitor tracking program utilities are AOL Instant Messenger, eBay, Friendster, Hi5, MySpace and Yahoo!360. The sites that do not support visitor tracking utility programs are Bebo, DeviantArt.com, Facebook, Netlog, Orkut, Perfspot and Zorpia.

Currently, creating a visitor log for Facebook using the Facebook programming API is against the Facebook Developer terms and conditions. Users who attempt to create an application which tracks profile hits without visitor knowledge will be banned from the site if the application is found. Recall the discussion in Section 7.6 – it is possible to retrieve the sender's IP address from an E-Mail you received at your Gmail, Hotmail and Yahoo mail accounts. The steps are presented in Table 7.8.

As a responsible Netizen, you can take a few basic precautions; for example, knowing more about the person communicating with you online can protect you. Owing to the increased amount of crimes being committed over the internet, knowing the true identity and location of others can add another layer of protection on the lighter side, see Fig. 7.25.

Details of tools used for digital forensics with each type of OS (Windows, Unix, MAC, etc.) can be studied by referring to technical books on cyber/computer/digital forensics. Some such books are mentioned in Refs. #1–10, Books, Further Reading. There are also links provided in Video Clips, Further Reading for video demonstrations. To conclude this section, we say that providing social networking site users with tools which will help protect them is ideal. Such tools are developed for installation on a user's computer to provide them the ability to retrieve other online user information via chat and social network websites. These tools will also benefit law enforcement agents when crimes are committed. Such tools typically help retrieve the IP address, OS (used on the machine from where the browsing is done) and the browser types associated with the used session for visiting a social networking site. Retrieval of this information occurs upon the virtual contact from that other person, be it by them simply browsing our personal page or by other person contacting via virtual meeting, for example chatting. Now let us understand computer forensics from compliance perspective.

7.15 Computer Forensics from Compliance Perspective

With the rampant use of the Internet, there is so much at stake; corporate data is not safe anymore given that almost all information assets lie on the corporate networks. We are in the era of Net-centric digital economy.



Criminals can gather small pieces about you, about your confidential data to generate what is known as "digital persona," that is, they keep track about your Internet activities, what resides on your corporate networks, etc.

Recall the discussion in Chapter 2 about how cybercriminals plan their attacks. There are cybercrimes and therefore there are investigations. Investigations require "evidences." This takes us to the legal territory where there are a number of legal compliance requirements. Information security compliance requires the precise enforcement of policies and controls. Investigations, in which computer forensics techniques are utilized, become an essential part of this enforcement. Let us revisit our thinking on the key information security laws and regulations that mandate computer forensics for compliance. It is appropriate to address this here in this section because we want to understand how the need for mandatory legal compliance can affect cyberforensics.

7.15.1 The Regulatory Perspective for Forensics at the International Level



Internationally, there are a few laws and regulations that indicate the need for digital investigations: *Sarbanes Oxley* (the SOX), *California SB 1386* (see Box 7.16), *Gramm Leach Bliley Act* (the GLBA) and *Health Insurance Portability and Accountability Act* (HIPAA) of 1996.

These laws/regulations specify investigation and response to security breaches or policy violations. Computer forensics makes it easier to meet these requirements.

IT businesses are “global” with customers and IT service supplier organizations operate all over the world. We focus on the aforementioned “Big-4 laws” (SOX, California SB 1386, the GLBA and HIPAA) because they have the broadest implications for commercial organizations. They impact companies that are publicly traded, store financial or medical information or do business in California. To illustrate the implication, let us say that there is a BPO center in India that deals with support to medical entities in California; as such the HIPAA may become relevant under regulatory compliance. Such business scenarios can affect most medium to large businesses as international companies that do business in the US. Such requirements can impact global businesses.

Let us understand the role of computer forensics in achieving compliance to the Big-4 laws mentioned. After recourse to these *Big-4 laws*, we shall examine computer forensics expertise situation in India with regard to the Indian ITA 2008. We will learn that through the requirement for “adequate security practices,” which include “security incident handling,” these laws/legislations become relevant in the context of forensics with cybercrimes.

Box 7.16 California Senate Bill 1386 (Another Angle to Cyberforensics)

The Bill is important for those involved in doing business with an entity in the US. California's first-of-its-kind information security legislation (SB 1386) went into effect on 1 July 2003. This legislation requires entities or individuals who do business in California to notify California residents whenever their unencrypted personal information is reasonably believed to have been compromised. According to California Senate Bill 1386, personal information includes “an individual's first name or first initial and last name in combination with one or more of the following”: a social security number, driver's license number or California Identification Card number, account number and/or credit or debit card information including numbers and passwords, PINs and access codes. The bill also limits coverage to personal data that is “unencrypted.” The statute provides a broad definition for “security breach” as an “unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the person or business.” The statute does not define the term “unauthorized” or specify what evidence of a breach is necessary to trigger notification obligations. The statute also does not resolve on the question whether companies have an affirmative duty to actively monitor and detect security breaches.

According to the Bill, it is mandatory for an organization to follow certain disclosure obligations following the discovery of a security breach that may have compromised customer data. “Notice must be given to any resident of California whose personal information is or is reasonably believed to have been acquired by an unauthorized person.” Notice must be given in “most expedient time possible” and “without unreasonable delay” subject to certain provisions that define what reasonable is for your organization. Organizations that hold personal data on California residents, it becomes essential for IT departments to review the security of consumers' personal information.

1. **The Sarbanes Oxley Act (SOX):** The Act was enacted to fight corporate fraud. Massive financial fraud at Enron, WorldCom, Global Crossing and Arthur Anderson led to the passing of this legislation in 2002. The Securities and Exchange Commission (SEC) is responsible for enforcement of SOX and all publicly traded companies must report yearly on the effectiveness of their financial controls. Corporate Governance has become a critical operational focus of organizations to ensure that they have the proper controls and audit processes in place to prevent and detect fraud.

The legislation has serious consequences for non-compliance. This includes civil and criminal penalties. Section 302 of SOX specifies that CEOs and CFOs are directly responsible for the accuracy of their company's financial reports. Much of the focus on SOX has been regarding Section 404. Section 404 requires management to specify their responsibility for financial controls and report on the adequacy and shortcoming of the controls. Many companies offer products and services to help companies achieve Section 404 compliance. SOX has other provisions that have not received the same attention from technology and service providers.

Many companies recognize the need for computer forensics as part of normal business operations and controls and it therefore indirectly supports Section 404 compliance. For Section 301, case law has established that computer forensics is required to properly investigate fraud. In addition, computer forensics is widely accepted as the only precise and reliable method to determine if digital records have been deleted and/or altered; therefore, computer forensics is needed to maintain compliance with Section 802 (this section of SOX impacts electronic evidence). Computer forensics has proven itself as a tool in fighting against wrongful termination litigation, HR investigations, *theft of intellectual property* and *E-Discovery management*; all of these issues enhance the accuracy of financial reporting, thus supporting Section 404. Sections 301 and 802 compliance will require the use of computer forensics as established by case law and by best practices. In today's world, it becomes essential for organizations to have computer forensics capability anywhere and anytime in their organizations to ensure compliance with Sarbanes Oxley.

2. **California SB 1386 (refer to Box 7.16):** This Bill requires organizations doing business in California to report security breaches that result in the unauthorized disclosure of a resident's private or financial information. The objective for this legislation is to thwart identity theft and consumer fraud. Given that many organizations (IT companies as well as non-IT companies) worldwide are engaged in business with the US, this law affects most domestic and international companies. Disclosure is required if an exposure to individual's "personal information" is involved (see Box 7.16). Notification, however, is not required if the information disclosed was encrypted.

The law allows for civil actions to be brought against non-complying businesses or they may be enjoined by the court. It is crucial for any business to conduct a thorough investigation to determine if it "reasonably" believes that information has been compromised or not. The legislation does not provide a clear definition for "reasonable investigation of a security breach." However, security organizations and government agencies have documented current incident response processes.

The National Institute of Standards and Technology (NIST) provides clear guidance for government and commercial organizations to investigate security incidents.^[20] NIST publication on the *Computer Security Incident Handling Guide*^[20] specifically outlines incident investigation and the role of computer forensics to properly acquire and analyze the incident. NIST also clearly identifies "unauthorized access" as a type of security breach that their process addresses.

3. **Gramm-Leach Bliley Act (GLBA):** This Financial Modernization Act of 1999 (known as the GLBA) has a broad spectrum of qualifications, requirements and regulating parties. Eight agencies and states are charged with managing and enforcing the regulations. The GLBA applies to financial organizations or any organization that collects or transfers private financial information for the purpose of doing business or providing a service to its customers.

There are two aspects of GLBA: (a) the *Financial Privacy Rule* and (b) the *Safeguards Rule*. The Financial Privacy Rule addresses the collection and dissemination of customers' information whereas the Safeguards Rule governs the processes and controls in an organization to protect customers' financial data. The Federal Trade Commission enforces the "Safeguards Rule" in GLBA. In addition to the public embarrassment of non-compliance, organizations may be fined thousands of dollars a day while they are non-compliant.

The Safeguards Rule of GLB calls for financial institutions to:

1. Ensure the security and confidentiality of customer information;
2. protect against any anticipated threats or hazards to the security or integrity of such information;
3. protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The GLBA is relevant to forensics because computer forensics is an integral part of investigating and auditing all of GLB Safeguards Rule elements mentioned above. For response to incidents, GLBA guidelines require – *"Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies."*

Technical guidelines that support GLBA call for extensive Intrusion Detection System (IDS) response by utilizing computer forensics investigations. To know more on IDS, refer to Ref. #17, Books, Further Reading. From the guidelines for security controls and the guidelines for incident response, we believe that GLBA compliance requires the utilization of computer forensics both proactively and for incident response to ensure the privacy of client information and to exhibit due diligence in GLB compliant efforts.

4. **HIPAA (Health Insurance Portability and Accountability Act of 1996):** HIPAA has the primary goal for healthcare providers to improve the privacy and security of their clients' medical information. In the US, healthcare providers (hospitals, medical insurance agents, medical professionals and many allied entities involved in delivery of healthcare services) records clearing houses and health plans must comply with HIPAA. Trading partner organizations that handle medical records electronically would fall under HIPAA rules.

Finalized HIPAA rules include "information security" which encompasses incident response. HIPAA definition of security incident is "... the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system." HIPAA specifies that there should be thorough analysis and reporting of security incidents – with that comes the need for the forensics investigation. Organizations must, therefore, consider their incident response policies carefully. Generally, such policies are part of organization's overall security policies; much about this is addressed in Chapter 9. Security policy and procedures aspects are addressed in detail in Ref. #13, Books, Further Reading.

Computer forensics software is often specified to be part of any reasonable incident response policy to clearly understand the scope of the incident. Determining, with forensics precision, what information has been compromised, when the compromise took place, what systems were affected, and if malware or backdoors (see Chapter 4) that are invisible to non-forensics tools are still present, are examples of the types of investigations that are essential to having an effective incident response program. Even beyond security incidents, computer forensics plays a natural role in supporting overall information security by providing the investigation of any anomalies that could indicate policy or use violations that could jeopardize HIPAA privacy rules.

Having understood why the Big-4 laws/legislations are important from the forensics compliance perspective, let us understand the changing face of computer forensics in terms of “traditional forensics” (see Fig. 7.26) vs. “remote forensics.” Basically, computer forensics requires accessing system data in a least-intrusive manner. Traditionally, this has meant removing the hard drive from the suspect computer and connecting it to a forensics workstation using a write blocker^[21] (Fig. 7.18).

Compliance requirements in the forensics field require that the (digital) evidence must be “forensically sound.” According to the literature,^[22] a forensically sound copy of a hard drive is as follows:

... created by a method that does not, in any way, alter any data on the drive being duplicated. A forensically sound duplicate must contain a copy of every bit, byte and sector of the source drive, including unallocated empty space and slack space; precisely as such data appears on the source drive relative to the other data on the drive. Finally, a forensically-sound duplicate will not contain any data... other than which was copied from the source drive.

Furthermore, it can be said that the manner used to obtain the evidence must be documented and should be justified to the extent applicable.

As learned in this chapter, one of the key requirements of a sound forensics examination of digital evidence is that the original evidence must not be modified, that is, the examination or capture of digital data from the hard disks of a seized computer must be performed so that the disk contents are not changed (recall the discussion in Sections 7.5 and 7.7). This is because, during forensics acquisition and analysis, it is possible to write to the evidence drive accidentally.

For example, in the US, there are “Federal Rules of Evidence”; to be admissible in a US court, evidence must be both relevant and reliable. The reliability of scientific evidence, such as the output from a digital forensics tool, is ascertained by the judge (as opposed to a jury) in a pre-trial “Daubert Hearing.”^[23] The Daubert Test is an expansion of the court’s prior approach to the admissibility of scientific evidence. To avoid the immediate dismissal of the evidence from court, the investigator should take care not to compromise the evidence.

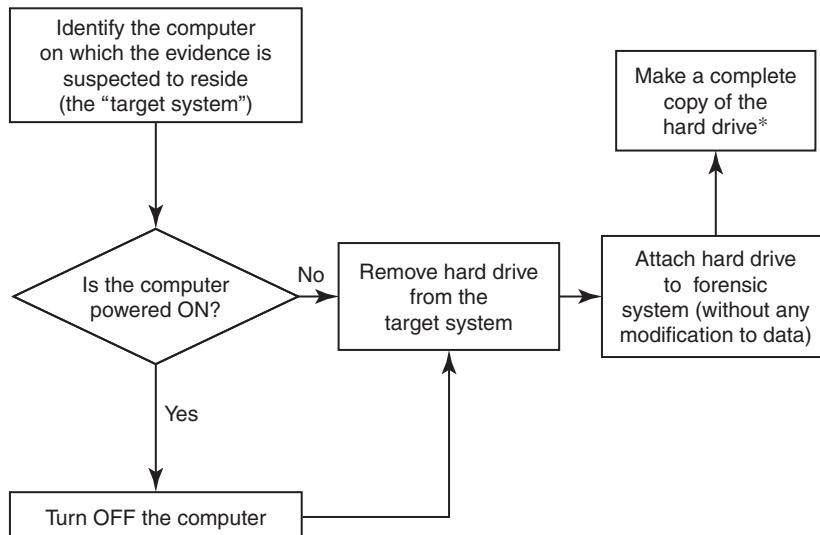


Figure 7.26 | Traditional approach to forensics analysis. *denotes tools/devices mentioned in Fig. 7.14.

The easiest way to ensure this is to use a *write blocker*. The investigator follows a set of procedures that are designed to prevent the execution of any program that would likely modify the disk contents. With the write blocker tool, the forensics investigator can examine the data on disk without alteration. There are several drawbacks with this methodology. First, it is costly and slow to physically remove the disk from a server, and the removal of the disk means downtime and user dissatisfaction. Second, although the data is not altered, important volatile data is lost because the system must be powered off to remove the disk. Although the investigator may utilize system tools and freeware to access this data before the system is shutdown, the data gathered is suspect as it may be compromised by malware running in the server. In other words, the “chain of custody” (the concept was explained in Sections 7.4 and 7.8, and Box 7.4) can be suspected/questioned when the digital evidence is admitted in the court.

Owing to these issues, a new generation of computer forensics tools^[22] has been developed with the capability to examine a live system through your corporate network. By placing a small read-only agent on the server, disk data and volatile system data can be accessed and imaged via the network. There are literature references^[24] (reports/articles, etc.) indicating that this methodology called “remote forensics,” though new, has been successfully utilized in some courts. With the new generation of network-enabled computer forensics, the investigations can be done quickly and at a lower overall cost than traditional computer forensics.

7.15.2 Computer Forensics Compliance Requirements: Implications for Evidential Aspects

Due to the current cyberspace scenario, there is an increasing need for evidence in organizations. There are rising cybersecurity threats as well as compliance needs (as part of security incidence response handling) for presenting the digital evidences/computer evidences. Good digital evidence is thus becoming a business enabler. In the face of the security threats, the incidents that follow and the need for forensics investigations, organizations are turning to logs to provide a continuous trail of everything that happens with their IT systems and, more importantly, with their data. Refer to Table D.II.13 in Appendix D.

Today there are many tools available that generate logs of different types from different sources; such logs allow organizations to generate a picture of the IT activity. Let us consider an example; if a disgruntled employee harbors the ill intention to steal data accesses, a database containing confidential information, there would likely be a log of that activity that can be reviewed to determine the who, what and when of the access to such a database. Such “logs of IT activity” provide the pieces of information and organizations can use those pieces of information to follow the paths of all of their users, bad intentioned or not. Managing these logs can benefit an organization in a number of ways. These logs offer situational awareness and thereby help organizations identify new threats as well as allow their effective investigation. Review of routine logs and detailed analysis of stored logs are beneficial for identifying security incidents, policy violations, fraudulent activity and operational problems shortly after they have occurred, as well as for providing information useful for resolving such problems. Refer to Table D.II.13 in Appendix D.

Considering that log management provides inherent benefits of log management, it is not surprising that log data collection and analysis are generally considered to be a security industry “best practice.” However, there are a number of regulations that mandate the collection, storage, maintenance and review of logs, turning log management from a “should do” to a “must do.” Some of these regulations draw on National Institute of Standards and Technology Computer Security Special Publications (NIST SP) toward detailed log requirements.^[25]

7.15.3 Computer Forensics Expertise Status in India

There is a rise in cybercrimes – recall the overview provided in Chapter 1. In Chapter 6 (Section 6.5) some of the challenges with regard to cybercrime scenario in India were described. With that as a background for this section, it can be inferred that in India, computer forensics is a much needed expertise. At the present, there seems to be a shortage of these skills. India seems to suffer from a two-fold problem: lack of availability of cyberforensics expertise as well as lack of awareness about cyberforensics/digital forensics/computer forensics. Involvement of cyberforensics in the day-to-day activities of individuals as well as corporations is going to increase due to the rising rate of cybercrimes in India (recall the Indian cybercrime data presented in Chapter 1 (Tables 1.1–1.4). ICT has been strongly rooted in India. India has a large youth population with computer usage going high. Due to this it is no surprise that cybercrimes rates are on the rise. This brings the need for increased use of cyberforensics for resolving both civil and criminal issues in India – for example, computer forensics can be used to investigate tax evasion of the accused ones.

To sum up this section, we note that compliance efforts require computer forensics investigation capabilities to investigate privacy and security incidents. The reach of computer forensics must be enterprise-wide and ideally, the response time should be immediate in order to demonstrate that the organization are utilizing best practices in managing and controlling their information security compliance. Organizations need to have a combination of in-house capability supplemented with external expert services. The fact remains that India does not have cyberforensics capabilities and the required manpower in tune with growth of ICT-related crimes and contraventions. Data breaches and cybercrimes in India cannot be reduced till we make strong cyberlaws. Cyberlaws of India need to be supported by sound cybersecurity and effective cyberforensics. In the absence of legal enablement of ICT systems in India, there is not much to expect. We need a good team of techno-legal experts who not only help in the drafting of good laws but also its amendments and enforcement.

7.16 Challenges in Computer Forensics

Although computer forensics has well-developed techniques, investigation of cybercrime is by no means easy. A microcomputer may have 200 GB or more storage capacity. There are more than 5.2 billion messages expected to be sent and received in the US alone per day. There are more than 3 billion indexed webpages worldwide. There are more than 550 billion documents online. Terabytes of data are stored on tape or hard drives. Therefore, looking for forensics evidence among these is like looking for the proverbial needle in the haystack! Over and above this, there is another challenge; most of existing tools and methods allow anyone to alter any attribute associated with digital data. The form of digital data to be analyzed is usually transformed in some way and always processed before scrutiny. Encryption is a major antiforensics technique and key word search can be defeated by renaming file names.

Cybercrime investigators are faced by the challenge of how to collect the specific, probative and case-related information from very large groups of files. They need to use approaches such as link analysis and visualization.^[27] They need to use enabling techniques for lead discovery from very large groups of files; typical techniques used to look for “patterns” are the techniques called text mining and data mining^[27] along with the techniques of intelligent information retrieval; all this is part of “data mining” which is a vast subject not within the scope of this chapter. Readers interested in learning about data mining may refer to Ref. #24, Books, Further Reading . Computer forensics must also adapt quickly to new products and innovations with valid and reliable examination and analysis techniques.

On the network forensics side, there are many challenges. The networks may span multiple time zones and multiple jurisdictions and this makes it necessary to use absolutely trusted timestamps (to ensure the authentication and integrity of timestamps for each piece of network evidence) and ensuring that all jurisdictions collaborate. Moreover, the network data will be available in both offline and real-time modes, the latter requiring the ability to capture and analyze data on the fly. The data could involve many different protocols and the amount of data could potentially be very large due to the increasing size of network bandwidth. A protocol could also involve multiple layers of signal (e.g., voice-over IP or VoIP, HTTP tunneling – for the discussion on tunneling protocols readers can refer to Ref. #15, Books, Further Reading). The current set of computer forensics tools will not be able to handle the real-time and data size/volume. Techniques are required for rapidly tracing a computer criminal's network activities (e.g., IP address) and for mapping a network's topology. There need to be a paradigm shift for network forensics techniques to analyze the rate and size of captured data.

The increasing volume of potential data to examine can create problem for law enforcement. Seizing all the computers at a search site and examining them at the deepest levels are the most significant factors contributing to the examination backlog and yet they are difficult to achieve. In order to alleviate this problem, new data intake and data reduction strategies must be implemented. It is always a good idea to adapt data acquisition strategies to the goals involved in each specific case. These strategies must also be pragmatic with regard to data volume and time constraints. Technological obsolescence must be recognized – yesterday's computer is not the equivalent of today's computer and is not even remotely similar to tomorrow's computer. Failure to recognize this will inevitably result in lost investigative leads and ineffective prosecutions.

Many forensics matters do not go to trial, especially in the business arena where a convincing set of data often suffices to induce an out-of-court settlement, or where investigative techniques are applied on a "need-to-know" basis, such as to determine whether internal or external corporate espionage or malicious activity has occurred. Experts may assist in preparing legal briefs, and they can be requested to provide sworn testimony and opinions in city, state and federal hearings conducted by legislative bodies and their commissions or task forces. They frequently work hand-in-hand with computer security teams to assist in the development of procedural, policy and control techniques to help prevent (or assist in mitigating) losses. Durations of forensics investigations vary; they may take a few hours in complex case analysis or a few days for simple cases, or the investigations can persist over the course of years for complex cases. Although some experts are engaged for the full range of investigative and testimonial tasks, those who are valued for their highly persuasive verbal skills and who can react well to on-the-spot challenges, may only review and present evidence prepared by other forensics computing specialists. Certain digital information, beyond the contents of the data itself, may be pertinent to case development. Such information can include the time and date stamps of files, folder structure hierarchies and message transmission tags. Real-time data collection efforts are more complex because they may need to address legalities and privileges involved in surveillance, and must avoid inadvertent damage claims (such as may occur when a server is made inaccessible for a period of time). Things to be wary of include alterations to the digital media that could occur when the electronic device is turned ON or OFF, and inadvertent activation of Trojan Horse or time-bomb malware that was left behind to corrupt data and confound forensics efforts. One caveat is that "you should only find what is actually there" however, ensuring this can involve the development and implementation of collection, blocking, prevention and tracking techniques. This is whereless evidence collection kits comprising of software and hardware tools, can be applied and these kits become useful.

7.16.1 Technical Challenges: Understanding the Raw Data and its Structure

In this section, our objective is to understand some of the technical aspects encountered in digital forensics analysis; only a few examples will be provided. Treating all the technical challenges and their greater details

is not within the scope of this chapter as digital forensics is a very large domain. The phases involved in digital forensics investigation (Section 7.7.2) should be kept in mind while going through the discussion here. Familiarity with the basic computer science fundamentals will help to appreciate the discussion in the following paragraphs. We explain only the technical aspects of data representation that a digital forensics investigator must understand.

There are two aspects of the *technical challenges faced in digital forensics investigation* – one is the “complexity” problem and the other is the “quantity” problem involved in a digital forensics investigation. A digital forensics investigator often faces the “complexity problem” because acquired data is typically at the lowest and most raw format. Non-technical people may find it too difficult to understand such format. For resolving the complexity problem, tools are useful; they translate data through one or more “layers of abstraction” until it can be understood. For example, to view the contents of a directory from a file system image, tools process the file system structures so that the appropriate values are displayed. The data that represents the files in a directory exist in formats that are too low level to identify without the assistance of tools.

The directory is a layer of abstraction in the file system. Examples of non-file system layers of abstraction include:

1. ASCII;
2. HTML Files;
3. Windows Registry;
4. Network Packets;
5. Source Code.

Digital forensics is also challenged by the “quantity problem” – it involves the hugeness of digital forensics to analyze. It is inefficient to analyze every single piece of it. Data reduction techniques need to be used to solve this. Data reduction is done by grouping data into one larger event or by removing known data. Examples of abstraction layers are data reduction techniques; for example:

1. Identifying known network packets using IDS signatures;
2. identifying unknown entries during log processing;
3. identifying known files using hash databases;
4. sorting files by their type.

Digital forensics analysis tools aim at accurately presenting all data at an appropriate layer of abstraction and format, so that the tools can be effectively used by an investigator to identify evidence. The required layer of abstraction is dependent on investigator's skill level as well as the investigation requirements. For example, in some cases viewing the raw contents of a disk block is appropriate whereas other cases will require the disk block to be processed as a file system structure. Tools must exist to provide both options. Let us understand the abstraction layer properties with regard to digital forensics. Large amounts of data are analyzed in a more manageable format using the abstraction layers. Abstraction of data layers is a core feature in the design of modern digital systems. This is because, all data, regardless of application, is represented on a disk or network in a generic format, bits that are set to one or zero. For using this generic storage format for custom applications, the data bits are translated by the applications to a structure that meets its needs. The custom format is a layer of abstraction.

ASCII is one basic example of abstraction. Every letter of the English alphabet is assigned to a number between 32 and 127 (for detailed information about ASCII scheme refer to the link <http://en.wikipedia.org/wiki/ASCII>). When a text file is saved, the letters are translated to their numerical representation and the value is saved on the media as bits. When the file is viewed in the raw, it shows a series of ones and zeros. When the ASCII layer of abstraction is applied, the numerical values get mapped to their corresponding

characters and the file is displayed as a series of letters, numbers and symbols. A text editor is an example of a tool operating at this layer of abstraction.

Next, let us consider fat file system example; “FAT” is a file allocation table. FAT file system is one of the most basic file systems that is still used in many computers. It is broken up into three main areas. The first area is the *Boot Sector* that contains the addresses and sizes of structures in this specific file system. The next two areas are the FAT and the *Data Area*. The locations of which are identified in the Boot Sector. The *Data Area* is divided into consecutive sectors called *clusters*. Clusters store the contents of a file or directory. Each cluster has an entry in the FAT that specifies if the cluster is unallocated or which cluster is the next in the file that has allocated it. Files are described by a *directory entry* structure. The directory entry structures are stored in the clusters allocated to the parent directory. The structure contains the file name, time, size and starting cluster. The remaining clusters in the file, if any, are identified using the FAT.

The FAT file system has seven layers of abstraction. The first layer uses just the partition image as input, assuming that the acquisition was done of the raw partition using a tool such as the UNIX “dd” tool. This layer uses the defined Boot Sector structure and extracts the size and location values. Examples of extracted values include:

1. Starting location of FAT;
2. size of each FAT;
3. number of FATs;
4. number of sectors per cluster;
5. location of Root Directory

The abstraction layers of the FAT file system are as follows:

1. Layer 0: Raw file system image;
2. Layer 1: File system image and values from Boot Sector and FAT Entry Size;
3. Layer 2: FAT Area and Data Area;
4. Layer 3: Starting Cluster, FAT Entries;
5. Layer 4: Clusters, Raw Cluster Content and Content Type;
6. Layer 5: Formatted Cluster Content;
7. Layer 6: List of Clusters.

Thus, we see that the digital forensics investigator has to have highly technical skills of understanding the data structure and its representation inside the computer systems where the digital evidence is suspected to reside.

7.16.2 The Legal Challenges in Computer Forensics and Data Privacy Issues



Evidence, to be admissible in court, must be relevant, material and competent, and its probative value must outweigh any prejudicial effect.

Although digital evidence is not unique with regard to relevancy and materiality, there is still a challenge involved. Digital evidence can be easily duplicated and modified; often it can be without even leaving any traces; it can present special problems related to competency. What is more to even reach the point where specific competency questions are answered, digital evidence needs to satisfy the legal admissibility

requirements. Modern computers have enormous data storage facilities. Gigabyte disk drives are common and a single computer may contain several such drives. Seizing and freezing of digital evidence can no longer be accomplished just by burning a single CD-ROM. Failure to freeze the evidence prior to opening the files, coupled with the fact that merely opening the files changes them, can and has invalidated critical evidence. There is also the problem of locating the relevant evidence within massive amounts of data. Examining such volumes of information to find relevant evidence is a daunting task. Owing to this, people often tend to think that there are complicated technical aspects in digital forensics. However, the reality is far from this. Although there are many technical aspects of digital forensics (recall the discussion in the preceding section), they involve understanding the raw data stored inside computer systems, retrieving data from existing or deleted files, interpreting their meaning and putting them within the context of the investigation. Actually, the real challenges involve artificial limitations imposed by constitutional, statutory and procedural issues – we often loose sight of the goal of retrieving evidence!



There are many types of personnel involved in digital forensics/computer forensics: (a) technicians, (b) policy makers and (c) professionals.

Technicians who carry out the technical aspects of gathering evidence. They have sufficient technical skills to gather information from digital devices, understand software and hardware as well as networks. The technical skills include – familiarity with computer hardware – thoroughly knowing the inside of the computer, understanding how hard drives work and their settings, understanding motherboards, understanding how the computer power supply units work and knowing about computer power connections, knowing how computer memory chips work (refer to Fig. 7.8). On the software side, the skills involve thorough understanding of various types of computer OS (e.g., Microsoft OS products, Linux, Unix. etc.), forensics products (diagnostic utilities and forensics diagnostic software and hardware equipment that are available in the market (see Tables 7.9–7.11)). In addition, professional forensics training is a must to enter this domain. They explain many technical aspects such as – difference between “clone” and “image” of drive, how do you make a “forensically sound” duplicate of a drive, how can you prove that the duplicate drive is forensically sound, steps to preserve the forensics evidence, etc. For technicians, forensics analysis of E-Mails is also important – it is explained in Section 7.6.

There are also *Policy Makers*; they establish forensics policies that reflect broad considerations – their main focus is on the big picture, but they must be familiar with computing and forensics also. The other entity involved in a digital forensics investigation is the *Professionals* – the link between policy and execution – who must have extensive technical skills as well as good understanding of the legal procedures. Skills for digital forensics professionals are the following:

1. Identify relevant electronic evidence associated with violations of specific laws;
2. identify and articulate probable cause necessary to obtain a search warrant and recognize the limits of warrants;
3. locate and recover relevant electronic evidence from computer systems using tools;
4. recognize and maintain a chain of custody;
5. follow a documented forensics investigation process.

To know more on technical details, legal professionals and those who are practicing in the cybercrime area may refer to Ref. #16, Additional Useful References, Further Reading.

Box 7.17 Drama in Court! Impact of Cyberforensics on Legal Practitioners

It would be no exaggeration to say that the public is primarily educated about forensics science by Hollywood films and television shows. There is no dearth of investigative news shows, documentaries, docudramas, Hollywood films and crime dramas that show us the horrifying and scary details of computer crimes. For example, on the popular YouTube media, there are hundreds of video clips available on these crimes. The media often focuses on law enforcement personnel who use "forensics" techniques to solve crimes. In a way, this is an update to the Sherlock Holmes crime investigation novels, as he used logic and scientific technique to single out the real suspect, often from a plethora of viable candidates. Probably the most popular recent movie series to focus on the use of forensics techniques are those based on the character of criminal, Hannibal Lector. Each of the three movies (*Silence of the Lambs*, *Red Dragon* and *Hannibal*) featured an FBI forensics profiler as one of its main characters.

In a scenario such as described above, an interesting question to explore is: Given the widespread popularity of forensics crime portrayals, do prosecutors and defense lawyers sense a change in jury expectations? Given the media's current emphasis on the importance of forensics science to resolve criminal investigations, a logical question to ask is if prospective jurors now have a higher expectation on the presentation of physical evidence by forensics experts. When criminal cases rely on testimonial and circumstantial evidence, do jury members feel that something is amiss? Is there a possibility that jurists might acquit when forensics evidence is not presented during a trial, but substantial circumstantial and testimonial evidence exists? If these changes are being perceived by attorneys as genuine, have lawyers reacted to changes in jurors by adjusting trial preparation and the presentation of evidence at trial? Additionally, are attorneys questioning jurors' viewing habits to either strike or attempt to retain avid viewers of forensics crime dramas?

Detection and recovery is the heart of computer forensics. This is the aspect which matters in the legal presentation of a cybercrime case in the court. The goal of detection and recovery is to recognize the digital objects that may contain information about the incident and document them. "Acquisition" is to copy and preserve the state of data that could be evidence. By "forensic acquisition of media" we mean the process of making a bit-for-bit copy, or image file, of a piece of media, where image files are frequently used in civil or criminal court proceeding. Therefore, completeness and accuracy of acquisition process is required. In addition, the source of evidence must remain and not get altered by attackers or by normal processes innocently.

Technical persons involved in digital forensics/computer forensics need simple technical skills such as understanding the various kinds of file systems (e.g., the FAT), system software, data organization and specific OS – Windows, Mac and Linux/Unix being the main operating systems in the market today. For the hand-held digital mobile devices there are operating systems such as the Symbian, the Palm OS, file systems and evidence recovery, etc. The legal professionals need to understand the working of court system, the legislations, laws (for cybercrime), and the investigative process and the evidential value of the electronic artifacts recovered/seized as potential evidences to be presented in the court while putting up the case.

Data of digital nature can be very easily deleted or altered; for example, by turning ON the computer or by simply opening/viewing a file or by password protecting files or even by saving data to another platform. Information may be available in areas that necessitate the use of special tools and techniques to identify and review. If data is not properly recovered and analyzed, it may not be admissible and/or credible in a court of law. Therefore, forensics investigators need to be careful in the matter of capturing the "perceived" evidence. They should understand that before they seize a computer or other electronic hardware they must consider whether they require a search warrant. They should be aware that if they wish to access stored electronic communications, they will need to comply with the Privacy Act/Privacy Law if applicable in their country. In order to conduct real-time electronic surveillance, they will need to obtain a wiretap order from a judge.

If access to digital evidence does not come through from an confiscation agency, court orders may become necessary to obtain the data as well as use of the extraction tools to determine whether protocols had been appropriately applied. Conversely, a prosecution or defense team may wish to suppress evidence from discovery, if they believe it could be damaging to the case. This is where the time-consuming aspects of the forensics examination may occur. In general, it is difficult to perform a comprehensive decomposition and logging of all materials (such as the contents of every sector of a terabyte hard drive, or thousands of hours of digital video from a surveillance camera), so a “scratch-and-sniff” approach might be used to yield promising information. Even though cost-effective, tactical decisions to proceed with only a partial investigation may be regretted in hindsight if a post-mortem comprehensive analysis shows that an alternative outcome might have prevailed.

Box 7.18 Beware – Forensics Acts and Laws!

It is said that forensics is a territory of dilemmas! The foremost dilemma with the study of electronic law is that it is very complicated to confine its study within simple parameters; Internet and electronic commerce do not define a distinct area of law as with contract and tort law. Electronic law crosses many legal disciplines, each of which can be studied individually. Cybercriminals abound – there will always be those in the world who wish to gain some benefit without actually paying for it. As a result, the electronic law will also cross-over certain aspects of criminal law.

In Chapter 1, many forms of cybercrimes are mentioned. Whether it is racial or sexual harassment, stalking, bullying at work or neighbors from hell, harassment is a form of discrimination that is generally prohibited by legislation. Harassment in the workplace is something employers must not tolerate, and includes any form of unwelcome, unsolicited, or unreciprocated behavior that a reasonable person would consider offensive, humiliating or intimidating. Chapters 1 and 2 mention about cyberstalking. Cyberstalking is the distribution of malicious communication through E-Mail and the Internet. Although based on new technology, it is in principle precisely the same as many other form of malicious communication and can be dealt with through the usual civil and criminal law methods. The distribution of offensive E-Mail through the Internet and such communication will also constitute an offense under a variety of statutes (such as the Malicious Communication Act in the UK).

Chapter 1 mentioned Children's Online Privacy Protection Act (COPPA). Pornography is a big business on the Internet and has even been seen by some as its foundation. In the US, pornography is protected as speech under the First Amendment of the Constitution. Obscenity, on the other hand, is not protected. Obscenity may be legally possessed in an individual's private home, but generally its distribution is illegal.

In much of the common law world, law enforcement needs to obtain a legal authorization in order to search and seize evidence. Generally, this power is granted through a request for a search warrant that states the grounds for the application, including the law that has been broken. In the US, the requirements demand that the application describe the specific premises need to be searched, as well as the items being sought. In the physical world, there is a real limit on the length of time during which a search can be conducted. This rule does not impose much of a limit on electronic searches. As investigators make a copy of the digital evidence (such as a hard drive), they are able to continue to search those files for “string,” which are beyond the scope of the original warrant, and do so at their leisure. According to the Fourth Amendment rule, an investigator executing a warrant is able to look in any place listed on the warrant where evidence might conceivably be concealed. Text of the Fourth Amendment states the following:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

As per traditional practices, an investigator was precluded from looking into any location beyond the area of the evidence he/she wishes to seize. Electronic evidence, however, may be stored anywhere. The result is that in an investigator can electronically look anywhere in search of digital evidence. For more details on the Fourth Amendment in the cyberspace, refer to the link mentioned

Box 7.18 Beware – Forensics . . . (Continued)

at the end of this box. Chapter 6 mentions about “evidence.” The Indian IT Act impacts the Indian Penal Code 1860, the Indian Evidence Act 1872, The Bankers’ Books Evidence Act 1891, The Reserve Bank of India Act 1934 (see Chapter 6) to make them in tune with the provisions of the IT Act. Electronic evidence in law is the legal recognition and evidential value in litigation of evidence in digital format. An Anton Piller order is a civil court order providing for the right to search premises and seize evidence without prior warning. In the US, the Business Software Alliance has used those orders as a remedy when they are attempting to stop illegal software use (termed software piracy) and copyright infringement to achieve the recovery of property.

Refer to the following URL mentioned for a complete presentation on the Fourth Amendment:
<http://law.uoregon.edu/faculty/shoar/docs/cc10/2010-fourthamendment.ppt> (7 September 2010).
 Also see the link in Ref. #6, Video Clips, Further Reading.

7.17 Special Tools and Techniques

We present in this section ready reckoner of forensics tools as well as some special techniques such as “data mining.” Forensics tools have also been mentioned in various sections of this chapter so far – for example “file carving” is mentioned in Box 7.10. Most of the “file carvers” tools operate by first looking for file headers and/or footers and then by “carving out” the blocks between these two boundaries. Outlook files with extension “jpeg” and MS Word files are fragmented and, therefore, appear corrupted or missing to a user using traditional data carving. “Disk duplication” equipments were mentioned in Section 7.11. Embedded memories inside the computer were mentioned in Section 7.7.2. Recall that Computer Online Forensics Evidence Extractor (COFEE) was mentioned in Box 7.1. Helix is another well-known tool for digital forensics investigation. Helix is a tool specially tailored for incident response, system investigation and analysis, data recovery and security auditing. It is attuned to experienced users and system administrators working in small-to-medium, mixed environments, where threats of data loss and security breach are high. Helix has two modes – pure Linux bootable live CD and the Windows mode, where it can be used *in vivo* on top of a desktop running Windows OS. Helix is available for download by E-Mail registration. For further technical details on Helix, visit <http://www.dedoimedo.com/computers/helix.html> (10 February 2010).

The list of carving tools is presented in Table 7.9. The list of reviewed tools is presented in Table 7.11. Cyberforensics expert Peter Stephenson, when asked, about how important tools are in digital forensics, responded by saying “... *Essentially, incident management is a forensics problem. That challenge demands a serious toolkit of computer forensic, network-enabled forensic, network forensics and analytical tools.*” In the words of another well-known forensics analyst Steve Hailey, “*If the tools being used are the mechanism to find evidence on a computing device, and several different tools can replicate the process, then it doesn’t matter what tools were used.*”

Most tools have the same underlying principles:

1. Creating forensics quality or sector-by-sector images of media;
2. locating deleted/old partitions;
3. ascertaining date/time stamp information;
4. obtaining data from slack space;
5. recovering or “undeleting” files and directories, “carving” or recovering data based on file headers/file footers;
6. performing keyword searches;
7. recovering Internet history information.

7.17.1 Digital Forensics Tools Ready Reckoner

The list of “carving” tools presented in Table 7.9 is divided in three main categories (a) data recovery (b) partition recovery and (c) carving. The associated websites are also mentioned for more information on these tools. Readers may like to re-visit Box 7.10.

Table 7.9 | List of carving tools

Sr. No.	Name of the Tool	Brief Description
<i>Data Recovery Tools</i>		
1.	Norton Disk Edit	The master boot record is required to boot your computer. Having a current backup of your master boot record is an excellent way to ensure that, in the event of a virus or hardware failure, you will be able to recover your system in the shortest amount of time possible.
2.	HD Doctor Suite	It is a set of professional tools used to fix firmware problem.
3.	SalvationDATA	To know more on this, visit http://www.salvationdata.com/data-recovery-equipment/hd-doctor.htm
4.	BringBack	This tool claims to have a program that can read the “bad blocks” of Maxtor drives with proprietary commands. To know more on this, visit http://www.salvationdata.com/
5.	RAID Reconstructor	It is a set of professional tools used to fix firmware problem.
6.	e-ROL	The tool offers easy to use, inexpensive and highly successful data recovery for Windows and Linux (ext2) operating systems and digital images stored on memory cards, etc. To know more on this, visit http://www.toolsthatwork.com/bringback.htm
7.	Recuva	To know more on this, visit http://www.toolsthatwork.com/bringback.htm
8.	Restoration	Recuva is a freeware Windows tool that recovers accidentally deleted files. To know more on this, visit http://www.piriform.com/recuva
9.	Undelete Plus	Restoration is a freeware Windows software that will allow you to recover deleted files. To know more on this, visit http://www.snapfiles.com/get/restoration.html
10.	R-Studio	Undelete Plus is a free deleted file recovery tool that works for all versions of Windows (95-Vista), FAT12/16/32, NTFS and NTFS5 filesystems and can perform recovery on various solid state devices. To know more on this, visit http://www.snapfiles.com/get/restoration.html
11.	Stellar Phoenix	To know more on this, visit http://www.undelete-plus.com/
12.	DeepSpar Disk Imager	R-Studio is a data recovery software suite that can recover files from FAT(12-32), NTFS, NTFS 5, HFS/HFS+, FFS, UFS/UFS2 (*BSD, Solaris), Ext2/Ext3 (Linux) and so on. To know more on this, visit http://www.data-recovery-software.net/
13.	Adroit Photo Recovery	Data recovery software services and tools to recover lost data from hard drive. Visit http://www.stellarinfo.com/
		It is a dedicated disk imaging device built to handle disk-level problems and to recover bad sectors on a hard drive. To know more on this, visit http://www.deepspar.com/
		This is a photo recovery tool that uses validated carving and is able to recover fragmented photos. Adroit Photo Recovery is able to recover high definition RAW images from Canon, Nikon, etc. To know more on this, visit http://photo-recovery.info/

(Continued)

Table 7.9 | (Continued)

<i>Sr. No.</i>	<i>Name of the Tool</i>	<i>Brief Description</i>
<i>Partition Recovery Tools</i>		
1.	Partition Doctor	It helps recover deleted or lost partitions (FAT16/FAT32/NTFS/NTFS5/EXT2/EXT3/SWAP). To know more on this, visit http://www.ptdd.com/index.htm
2.	NTFS Recovery	DiskInternals NTFS Recovery is a fully automatic utility that recovers data from damaged or formatted disks.
3.	gpart	To know more on this, visit http://www.diskinternals.com/ntfs-recovery/ Gpart is a tool which tries to guess the primary partition table of a PC-type hard disk in case the primary partition table in sector 0 is damaged, incorrect or deleted.
4.	TestDisk	To know more on this, visit http://www.cgsecurity.org/wiki/TestDisk
5.	Partition Recover Software	This is an OSS tool (open-source software) and is licensed under the GNU Public License (GPL). Partition Recovery software for NTFS and FAT system that examines lost windows partition of damaged and corrupted hard drive.
		To know more on this, visit http://www.stellarinfo.com/partition-recovery.htm
<i>File Carving Tools</i>		
1.	DataLifter® - File Extractor Pro	Data carving runs on multiple threads to make use of modern processors. Visit http://www.datalifter.com/products.htm
2.	Simple Carver Suite	This is a collection of unique tools designed for a number of purposes including data recovery, forensics computing and E-Discovery. The suite was originally designed for data recovery and has since expanded to include unique file decoding, file identification and file classification. Visit http://www.simplecarver.com/
3.	Foremost	Foremost is a console program to recover files based on their headers, footers and internal data structures. Visit http://foremost.sourceforge.net/
4.	Scalpel	Scalpel is a fast file carver that reads a database of header and footer definitions and extracts matching files from a set of image files or raw device files. Scalpel is filesystem-independent and will carve files from FATx, NTFS, ext2/3, or raw partitions. Visit http://www.digitalforensicssolutions.com/Scalpel/
5.	CarvFs	A virtual file system (fuse) implementation that can provide carving tools with the possibility to do recursive multi-tool zero-storage carving (also called in-place carving). Patches and scripts for scalpel and foremost are provided. Works on raw and EnCase images. For more information, visit http://www.forensicswiki.org/wiki/CarvFs
6.	LibCarvPath	A shared library that allows carving tools to use zero-storage carving on carvfs virtual files. For more information, visit http://www.forensicswiki.org/wiki/LibCarvPath
7.	PhotoRec	This is file data recovery software designed to recover lost files including video, documents and archives from hard disks and CDROM and lost pictures (thus, its "Photo Recovery" name) from digital camera memory. Visit http://www.cgsecurity.org/wiki/PhotoRec

(Continued)

Table 7.9 | (Continued)

<i>Sr. No.</i>	<i>Name of the Tool</i>	<i>Brief Description</i>
8.	PhotoRescue	Datarescue PhotoRescue Advanced is picture and photo data recovery solution made by the creators of IDA Pro. PhotoRescue will undelete, unerase and recover pictures and files lost on corrupted, erased or damaged compact flash (CF) cards, SD Cards, Memory Sticks, SmartMedia and XD cards. For more information, visit http://www.datarescue.com/photorescue/
9.	RevIt	RevIt (Revive It) is an experimental carving tool, initially developed for the DFRWS 2006 carving challenge. It uses “file structure-based carving.” Note that RevIt currently is a work in progress. For more information, visit https://www.uitwisselplatform.nl/projects/revit
10.	Magic Rescue	Magic Rescue is a file carving tool that uses “magic bytes” in a file contents to recover data. For more information, visit http://www.student.dtu.dk/~s042078/magicrescue/
11.	FTK	FTK2 includes some file carvers. <i>Note:</i> see Table 7.11
12.	SmartCarving	SmartCarving is a file carving technique to recover fragmented files. SmartCarving utilizes a combination of structure-based validation along with validation of each file’s unique content.
13.	GuidedCarving	This is a technique to recover fragmented files introduced in <i>Adroit Photo Forensics</i> . GuidedCarving allows a user to attempt to recover a fragmented file that failed to fully recover using SmartCarving.
14.	Adroit Photo Forensics	Adroit Photo Forensics supports data carving of popular image formats. Also supports fragmented carving using <i>SmartCarving</i> and <i>GuidedCarving</i> .

Note: The term “Data Recovery” is frequently used to mean forensics recovery, but the term really should be used for recovering data from damaged media.

The information in Table 7.10 is based on Dr. Peter Stephenson’s in-depth review of forensics tools conducted in year 2006. The survey by Dr. Stephenson is considered to be one of the best known among similar other surveys. Links for other survey are mentioned after the table.

Prices indicated are “as at point in time” that is the exact prices should be found out at the time of purchase. Versions indicated are as per testing done in 2006 – for more information, refer to website www.scmagazine.com

Links to other surveys/reviews about forensics tools are provided below:

1. *Best Forensics Tools – 2007 Edition* can be accessed at the following link: <http://www.dragoslungu.com/2007/04/17/best-forensics-tools-2007-edition/> (4 April 2010).
2. *EnCase Forensic 6 – Review* is available at the following link: <http://whereismydata.wordpress.com/2008/08/31/encase-forensic-6-review/> (3 April 2010).
3. The following link will take you to *Computer Forensics Tool Testing (CFTT) Survey*: <http://blogs.sans.org/computer-forensics/2010/03/04/computer-forensics-tool-testing-cftt-survey/> (1 April 2010). Table 7.11 provides information about the tools compared in Table 7.10. Reference websites are also provided.

Table 7.10 | Forensics tools features comparison at a glance

<i>Product Name</i>	<i>Coroner's Toolkit</i>	<i>Encase Forensics Toolkit</i>	<i>Forensics Notebook</i>	<i>i2 Analyst's Log</i>	<i>LX2000 First Response</i>	<i>Mandiant NetWitness Incident Response</i>	<i>ProDiscover</i>	<i>Sleuth Kit/Autopsy Browser</i>
Supplier	Open source	Guidance software	Access data	i2Inc.	LogLogic	Mandiant	Man Tech Intl.	Technology Partners
UNIX/Linux platform	Yes	No	No	Yes	No	Yes	No	Open source
Windows Platform	No	Yes	Yes	No	Yes	No	Yes	Yes
Analyzes W – Windows U	U	W, U	W, U	—	W	—	W, U	W, U
U – UNIX/Linux	—	—	—	Yes	Yes	—	—	—
Remote Capture	No	No	No	—	Yes	—	Yes	No
GUI	No	Yes	Yes	Yes	Yes	No	Yes	Yes
Requires Remote Agent	No	No	No	No	Yes	No	No	No
Preforensics Audit	No	Yes	Yes	No	No	Yes	No	No

Table 7.11 | Top tools in digital forensics

<i>Name of the Tool</i>	<i>Brief Information</i>
The Coroner's Toolkit (TCT) Version 1.16 Visit www.porcupine.org	<ul style="list-style-type: none"> • OSS tool (open-source software) • No cost – OSS • Not a GUI-based product • Used with UNIX platform – it is a collection of command line tools • Written by Dan Farmer and Wietse Venema • Deep UNIX knowledge is the prerequisite to use TCT because it is a UNIX-only tool • Documentation is not detailed • Support to this tool is not much available – like most OSS tools, users are expected to fend for themselves
EnCase Forensics Version 5.0 Visit www.guidancesoftware.com	<ul style="list-style-type: none"> • GUI-based • Expensive • Adequate documentation • Simple to operate and use • Can acquire many different media • Plenty of web support • Costs around \$3000 Targeted at large organizations
Forensics Toolkit (FTK) Version 1.61 Visit www.accessdata.com	<ul style="list-style-type: none"> • Comprehensive with many features but not simple to use • Overwhelming program interface • Good documentation • Comes with a USB-pluggable hardware device • Costs around \$1100
i2 Analyst's Noted Version 6.0.55 Visit www.i2inc.com	<ul style="list-style-type: none"> • Very different type of forensics analysis tool • Can import metadata from EnCase • Data can be imported from spreadsheet using CSV file • Has the ability to analyze complex crimes • Help system is very good • People-based support is expensive (online support and phone support is also available) • Costs around \$3700
LogLogic's LX 2000 Visit www.loglogic.com	<ul style="list-style-type: none"> • Highly expensive – costs around \$50000 • Excellent tool for log analysis – analyzes logs in real-time mode • Mature and useful product • High functionality but complex to set up • Excellent interface but high learning curve (many hidden features to be understood) • Adequate documentation
Mandiant First Response Version 1.1 Visit www.mandiant.com	<ul style="list-style-type: none"> • No cost – freeware forensics audit tool with strong audit features • Not easy to use – awkward interface • Useful features once understood • Gathers forensics information in an organized and simple-to-read fashion • Limited support and limited documentation • Deploys agents across network computers to gather a snapshot before evidence is gathered

(Continued)

Table 7.11 | (Continued)

<i>Name of the Tool</i>	<i>Brief Information</i>
NetWitness Version 6.0 Visit www.netwitness.com	<ul style="list-style-type: none"> • Network traffic security analyzer and works as a security intelligence tool. Helps automate IDS analysis process • Good user interface • Set up is easy due to installation wizard • Good user interface • Low scalability • Inadequate documentation • Web-based support and E-Mail-based support for registered users • Costs \$30,000 • Not suitable for large enterprises
ProDiscover Incident Response Version 4.55 Visit www.techpathways.com	<ul style="list-style-type: none"> • Complete IT forensics tool can access computer over the network • Fairly easy to use • Supports remote analysis of running processes, open files, open port and services running on open ports • Not for first time users – experience in forensics required • Well laid-out documentation • Full disk imaging capability, ability to find hidden data, file metadata information, hash keeping as well as across network data gathering • Costs \$8000
Sleuth Kit and Autopsy Browser Visit www.sleuthkit.org	<ul style="list-style-type: none"> • No cost – it is a freeware • Good documentation • Good support • Straightforward to use for those familiar with UNIX environment but difficult to use by those not familiar with UNIX • Can use Non-UNIX file systems too • The browser can run on any HTML environment • Adequate documentation • Support is much better as compared to many other OSS – E-Mail-based support is available and many active user forums are available

7.17.2 Special Technique: Data Mining used in Cyberforensics

Data mining is a very vast topic; full treatment of this topic is beyond scope of the chapter. In this section, we are only going to explain how data mining techniques are applied in cyberforensics. Chapter 1 presents the various categories of cybercrimes. A criminal act can encompass a wide range of activities, from civil infractions such as illegal parking to internationally organized mass murder such as the 9/11 attacks in New York, US and 26/11 attacks in Mumbai, India. Law enforcement agencies across the world compile crime statistics. Depending on the type of cybercrimes, the impact and the impacted parties can vary. Some examples of impact and impacted parties are national security and government, financial impacts and individuals, brand image and organizations. More on this is presented in Chapter 9.

Traditional data mining techniques such as association analysis, classification and prediction, cluster analysis, and outlier analysis identify patterns in structured data. To know more on these analyses, visit <http://www.theairling.com/glossary.htm>. Newer techniques identify patterns from both structured and unstructured data. Literature^[28] shows that as with other forms of data mining, crime data mining raises privacy concerns. Automated data mining techniques are being researched for both local law enforcement and national security applications. A brief explanation of some of the data mining techniques is as follows:

1. **Entity extraction:** This technique is used to identify particular patterns from data such as text, images or audio materials. It has been used to automatically identify persons, addresses, vehicles and personal characteristics from police narrative reports.^[29] In computer forensics, the extraction of software information such as the data structure, program flow, organization and quantity of comments, and use of variable names, can facilitate further investigation by grouping similar programs written by hackers and tracing their behavior. Entity extraction technique provides basic information for crime analysis, but its performance depends greatly on the availability of extensive amounts of clean input data.
2. **Clustering techniques:** This involves grouping data items into classes with similar characteristics to maximize or minimize intraclass similarity. For example, in order to identify suspects who conduct crimes using similar methods or to distinguish among groups that belong to different gangs. These techniques are not featured with a set of predefined classes for assigning items. The statistics-based *concept space algorithm* is used to automatically associate different objects such as persons, organizations and vehicles in crime records.^[30] The Financial Crimes Enforcement Network AI System (AI is the branch of computer science, known as “Artificial Intelligence”)^[31] uses link analysis techniques (to identify transactions’ patterns) to exploit Bank Secrecy Act data to support the detection and analysis of money laundering and other financial crimes. The technique of “clustering” crime incidents can automate a major part of crime analysis but is limited by the high computational intensity typically required.
3. **Association rule mining:** This technique discovers frequently occurring item sets in a database and presents the patterns as rules. This technique has been applied to detect network intrusion and to derive association rules from users’ interaction history. Investigators can also apply this technique to network intruders’ profiles to help detect potential future network attacks.^[32]

Automated techniques to analyze different types of crimes need a unifying framework describing how to apply them. In particular, there is a need for understanding the relationship between analysis capability and crime type characteristics. This understanding can help investigators more effectively to use those techniques to identify trends and patterns, address problem areas and even predict crimes. After having completed a brief overview of data mining techniques in cyberforensics, we now discuss forensics auditing.

7.18 Forensics Auditing



“Forensics auditing” is also known as “forensics accounting.”

Forensic auditing includes the steps needed to detect and deter fraud. Forensics auditors make use of the latest technology to examine financial documents and investigate white-collar crimes like such as frauds, identity theft, funds embezzlement, securities fraud, insider trading, etc. Forensics accounting is a specialized form of accounting; it uses accounting, auditing and investigative techniques. Forensics accounting professionals are assigned specialty tasks, such as analyzing and tracking evidence of economic transactions. In some cases, they are asked to present this evidence to a court of law. Forensics auditors are responsible for detecting fraud, identifying individuals involved, collecting evidence, presenting the evidence in criminal proceedings, etc. From career perspective, forensics auditors can work in both large and small organizations like insurance companies, banks, courts, government agencies and law firms. Cybersecurity Careers are addressed in Chapter 12.

There is almost always some legal/evidential angle in forensics auditing. Consider as an example of forensics auditing, the investigation of a fraud or presumptive fraud with the objective of gathering evidence that could be presented in a court of law. There is an increasing use of auditing skills to prevent fraud by identifying and rectifying situations that could lead to frauds being perpetrated (i.e., risks). It might be useful, therefore, to categorize forensics auditing as being either “reactive” or “proactive.”

“Insider trading” needs some explanation. According to the American Heritage Dictionary, “insider trading” is the illegal buying or selling of securities on the basis of information that is unavailable to the public. It involves trading of a corporation’s stock or other securities (e.g., bonds or stock options) by individuals with potential access to non-public information about the company.

“Insider trading”^[33] refers to two separate financial transactions – one being perfectly legal and the other being subject to massive civil fines and possible prison time. There is a legal form of insider trading – it involves the sale of securities or stocks by officers of a company or stockholders who own more than 10% of the company. In many countries, trading by corporate insiders, for example, officers, key employees, directors and large shareholders, etc., may be considered legal if this trading is done in a way that does not take advantage of non-public information. However, the term is frequently used to refer to a practice in which an insider or a related party trades based on non-public information obtained during the performance of the insider’s duties at the corporation, or otherwise in breach of a fiduciary or other relationship of trust and confidence or where the non-public information was misappropriated from the company.

Recall the discussion about regulatory perspective for forensics (Section 7.15.1). Government departments/agencies can possibly use the techniques of forensics auditing to assess compliance with regulations governing payments of grants/subsidies. Compliance auditors could also use these techniques while auditing such governmental programs. We have mentioned about “steganography” in Section 7.12. Antiforensics tools can hide data with cryptography or steganography. “Antiforensics” is addressed in the next section. Although steganography has not yet come either under the direct scope of IT Audits or under cyberforensics investigation, because it is not yet considered a direct threat by auditors and cyberforensics investigators, it is the one that needs to be considered and understood for possible future occurrences.

Box 7.19 Auditing vis-à-vis Cyberforensics Investigation

For many people, both the terms auditing and cyberforensics investigation are the same but actually they are not. Typically, an “audit” involves examination of information and operations for accuracy, legality and propriety. Internal audits are meant to report risks and to make recommendations to promote sound-operating practices. Audit examinations typically involve documents, records, reports, internal control systems, accounting procedures and actual operations. On the other hand, “cyberforensics investigation” is the process of extracting information and data from computer storage media and guaranteeing its accuracy and reliability (typically in an evidential context).

Box 7.19 Auditing vis-à-vis . . . (Continued)

Objective of an “audit” is to determine whether all transactions are properly recorded in the accounts, and appropriately reflected in the organization’s statement and reports. The objective of a “cyberforensics investigation,” on the other hand, is to identify “digital evidence” using scientifically derived and proven methods that can be used to facilitate or to help reconstruct events in an investigation. The secondary objective is to identify the responsible person and seriousness of the misconduct.

Auditing and cyberforensics investigation vary in their “scope” too. Scope of an audit typically includes – audit objectives, risk assessment, nature and extend of controls testing (compliance testing or substantive testing) and the extent of auditing procedures to be performed, reliance on previous audits. The scope of cyberforensics investigation involves scientific methods to identify, collect, analyze, validate, interpret, preserve, document and present electronic evidence derived from digital sources.

Results of audit are generally communicated via written report to management. On the other hand, report of a cyberforensics investigation is submitted to the investigator, prosecutor, law enforcement, organizational management and others. The impacts differ too. An audit is conducted in a non-confrontational manner, with generally helpful cooperation by the auditee whereas a cyberforensics investigation may be adversarial. Each investigation is independent and unique in itself.

Recall the discussion in Section 7.5.1 The Rules of Evidence – “secure, auditable digital date/time stamps” will have the following attributes:

1. **Accuracy:** The time presented is from an authoritative source and is accurate precision required by the transaction, whether day/hour/millisecond.
2. **Authentication:** The source of time is authenticated to a suitable timing laboratory so that a third party can verify the precision and accuracy.
3. **Integrity:** The time should be secured and not subjected to corruption during “handling.” If it is corrupted, either inadvertently or deliberately, the corruption will be apparent to a third party.
4. **Non-repudiation:** An event or document should be bound to its time so that association between event or document and the time cannot be later denied.
5. **Accountability:** The process of acquiring time, adding authentication and binding it to the subject event should be accountable, so that a third party can be assured that due process was applied and that no corruption transpired.

“Digital Evidence Collection” is a game of patience. The potential for fraud, unintended errors can be eliminated by adding secure and auditable time to digital evidence. The use of secure date/time stamps can not only improve the integrity digital evidence, but also provide higher assurance required for digital chain of evidence. Using secure and auditable time helps to ensure that any important electronic time stamp that cannot be corrupted has an evidentiary trail of authenticity. The secure issuance of timestamps for digital evidence has some critical components associated with them:

1. First, it must be remembered that digital data needs binding of time. Such binding of time with digital data must occur within a trusted computing environment to assure the “efficacy of the time stamping process.”
2. Next, it is important to consider the accuracy of the clock used as the source for time stamping. The clock used should be appropriate for the application. For example, the accuracy of a timestamp

indicating access to a secure facility through the use of a card access or biometric device of 30 seconds may be reasonable. However, the time stamp on an electronic stock transaction or money transfer may warrant a finer resolution.

3. When a local trusted clock is used as the source for time stamping, its calibration and audit must be routine, continuous and traceable. Furthermore, to make the audits reliable, the audit of such clocks must be performed by a trusted, disinterested third party.
4. Finally, the issuer must verify the validation of the resulting timestamps. The verification/validation records ought to be made available to any party that has the need to evaluate the accuracy, validity, trustworthiness or traceability of a timestamp.

7.19 Antiforensics

“Antiforensics” is the application of scientific method to digital media to invalidate factual information for judicial review. There are four categories of antiforensics: (a) *Data destruction*; (b) *data hiding*; (c) *data encryption* and (d) *data contraception*. Antiforensics is a combination of people, process and tools. There are several counter-forensics commercial software tools available in the market. They are designed to eliminate specific records and files but leave system otherwise functional, that is, overwrite deleted data to thwart recovery and cope with system files, like the Registry. Counter-forensics tools are increasingly reported as important factors in legal action. Organizations must seek to understand the mindset, skill set and capabilities of those employing antiforensics techniques. By way of a situational context, this is like trying to understand from cyberattackers’ perspective so that threats posed to the information systems can be understood. Cybercriminals exploit the fact that forensics takes time. Recall “Locard Exchange Principle” (Box 7.5) – conventional wisdom tell us that an attacker will attempt to leave as little evidence as possible. From another angle, however, there are significant advantages to an attacker for creating extraneous evidence. The first is the time factor mentioned earlier; forensics investigation takes time and time is money! Multisystem compromises against enterprise networks resulting in non-linear increase in the amount of effort that goes in accurate analysis of suspect system. In situations where an extraordinarily large number of computers are under suspicion, businesses can rarely perform a full forensics analysis of all the computers.

Recall the discussion in Section 7.16.2. In that context, here is another point on forensics from “privacy” perspective: Modern OS and applications that run on the OS generate a high amount of data about users’ activities. Current trends in computer use raise concerns about recovering “privacy-sensitive” data from computer systems, especially given the mobile computing trends and “remote working” trends. The line between “home” and “office” is getting thinner as work takes place round the clock in a “work anywhere” and “any time” mode. Employees use company computers (desktops, laptops, etc.) for personal E-Mails, banking, shopping, listening to music, watching video, etc. (although some organizations have strict rules and guidelines on allowed usage and security restrictions on sites to be visited using company computers). Refer to Chapter 9 and Appendix C.

When companies provide employees with laptops to work from home,^[34] other family members may also use these computers. In such a scenario, company computers often may contain “sensitive personal information” (along with business confidential information) which individuals want to keep private. The laptops may also contain records that companies would like to protect and examine. Users are getting increasingly aware of their “privacy exposure” from these records and the “digital artifacts” that linger even after files are “deleted” on the computer they use. As a result of this, a range of “counter-forensic” privacy tools have emerged. These tools are nothing but software designed to irretrievably eliminate records of

computer system usage and other “sensitive data.” Following are some of the lists of well-known tools with “counter-forensics features”:

1. Windows Washer;
2. Windows and Internet Cleaner;
3. CyberScrub Pro;
4. Evidence Eliminator;
5. Acronis Privacy Expert;
6. SecureClean.

A table^[35] showing feature comparison of 1, 2, 3 and 4 is available in a link in References. However, those are not the only antiforensics tools available in the market place today. More are described in the next paragraph.

Metasploit antiforensics investigation arsenal includes tools such as (a) *timestomp*,^[36] (b) *Slacker*, (c) *transmogrify* and (d) *Sam Juicer*. Let us first understand how “timestomp” acts as an antiforensics tool. Timestomp uses Windows system calls *NtQueryInformationFile()* and *NtSetInformationFile()*. However it does not use the call *SetFileTime()*. Timestomp features include display and set MACE attributes to mess up with EnCase and MS Anti-Spyware. Timestomp leverages a series of Win32 system calls to modify the Last Modified (M), Last Accessed (A), Creation Date (C) and Entry Modified (E), together referred to as “MACE.” During a forensics analysis, the examiner will use these values to attempt to piece together a timeline of event. If an attacker is able to undetectably modify these entries then the examiner can no longer rely on timestamps to create a timeline for the crime committed. By performing a series of standard Win32 function calls, an attacker can place data at the end of a cluster. A subsequent series of function calls allows an attacker to retrieve the stored data. Timestomp allows the techie criminal to hide information on a system that may not be immediately distinguished from other random slack space information. Little can be done to examine hidden slack space information that has been properly obfuscated or encrypted. This explains how “timestomp” may permit an attacker to subvert file time stamps to corrupt a forensics analysis; however, it can also be used to validate various forensics tools for reliability. Thus, it works like a double-edged sword!

“Transmogrify” is a simple search and replace engine that allows for the file signatures to be changed between various types. An attacker might change a JPG file to show up as a Windows Executable. Most popular forensics tools only perform the most basic pattern matching and file extension examination to identify file type. Therefore, an investigator relying on these tools is most likely to misidentify the file type and allow it to go as unexamined! The only way to tell if a file is a JPG would be to open it, and the only way to determine if a file is an EXE would be to execute it. This is because a JPG hidden as an EXE would never run and an EXE hidden as a JPG would never display!

Timestomp and *transmogrify*, mentioned in the previous paragraphs, are tools that focus on changing, hiding or planting misleading evidence. “Sam Juicer” is designed to help advanced attackers to prevent evidence from ever being created. As a result, no evidence will ever come to disk and, therefore, a postmortem forensics analysis of the disk will not reveal any clues as to how the compromise occurred. The analysis will not even throw light about the extent of control the attacker had on the computer system. There is no easy solution (as at the time of writing this) available to prevent Sam Juicer from running once the machine has been compromised.

A well-known tool, which is used for data hiding, is called *Slacker*^[37] – it is part of the Metasploit framework mentioned earlier in the section. Slacker can hide data within the slack space of FAT or New Technology File System (NTFS) file system. Slacker breaks a file into pieces and places each piece of that file into the

slack space of other files, thereby hiding it from the forensics examination software. At the beginning of this section, we mentioned that there are four categories of antiforensics – data hiding is one of those categories. Data hiding technique involves the use of bad sectors. When performing this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster. It is a common belief that forensics examination tools will see these clusters as bad and continue without any examination of their contents.

Forensics tools “Sleuth Kit” and “EnCase” are mentioned in Section 7.10 and Sections 7.7.2 and 7.10.2, and Tables 7.10 and 7.11 describe their features. EnCase relies on the Windows API to perform timestamp translation. However, a glitch in the Windows API results in a blank value being displayed when the time stamp values are set below a certain threshold. Thus, we need to appreciate

that computer forensics tools are neither panacea nor magic; after all, they are only complex software tools that like all software may be subject to certain attacks. Although these tools play such a critical role in our legal system, it is important that they be as accurate, reliable and secure against tampering as possible. Vulnerabilities would not only question the admissibility of forensics images, but could also create a risk that if undetected tampering occurs, courts may come to wrong decisions in cases that affect lives and property. Antiforensics is more than a technology. This approach to criminal hacking can be summed as follows: *Make it hard for them to find you and impossible for them to prove they found you*. If an attacker succeeds in making a cyberforensics investigation extremely costly, then he/she can actually create a business case against in-depth forensics analysis!

SUMMARY

The field of digital forensics/computer forensics has grown rapidly in the 21st century, most notably due to the increased trend in mobile devices found at technical, non-technical and violent crime scenes and the rise in mobile workforce in the global economy. Mobile computing/remote working, etc. are some of the emerging patterns of work. In this chapter, fundamentals of cyberforensics and its associated aspects were presented. Cyberforensics has become an important domain given the kind of world in which we live now and the way businesses now operate. Cybersecurity has become a mission-critical component in modern times. When security threats are not analyzed effectively, the result can be unpredictable catastrophes. The emergence of information forensics comes from the incidence of criminal, illegal and inappropriate behaviors. We are living in the knowledge age where information and knowledge are the most sought after commodities. Criminals, competitors and even employees exploit loopholes in current security architectures and control structures; use antiforensics techniques and tools to hide their

traces; and apply forensics tools and techniques to obtain the required information to commit cybercrimes. Steganography is a dynamic tool with a long history and the capability to adapt to new levels of technology. As steganographic tools reach the stage of advanced technological features, the steganalyst and the tools they use must also advance. In reference to steganography used by cybercriminals, we also explained about rootkits, which is a set of software tools inserted by an intruder into a computer in order to allow that intruder to enter the computer again at a later date and use it for malicious purposes without being detected. These purposes include (a) collecting data about computers (including other computers on a network) and their users (such as passwords and financial information), (b) causing such computers to malfunction and (c) creating or relaying Spam. Like any tool, steganography (and steganalysis) is neither inherently good nor evil; it is the manner in which it is used which will determine whether it is a benefit or a detriment to our society.

Security has become a major concern on social networks. It is very important that we find the right solutions to tackle the different security problems on the social networking sites today. The chain of evidence and accuracy of digital evidence is very important in cyberforensics investigation. Experienced human investigators can often analyze crime trends precisely, but as the incidence and complexity of crime increases, human errors occur, analysis time increases and criminals have more time to destroy

evidence and escape arrest. By increasing efficiency and reducing errors, crime data mining techniques can facilitate police and enable investigators to allocate their time to other valuable tasks. Attackers' objective is to make forensics investigation difficult. They aim at foiling the investigations. Antiforensics behaviors, tools and technologies are, therefore, an area of concern when they do not get caught, as discussed in the chapter.

REVIEW QUESTIONS

1. Is there a difference between computer security and computer forensics? Explain.
2. Can a cybercrime investigation be done without involving a forensics expert? Explain with reasons.
3. Explain how the “chain of custody” concept applies in computer/digital forensics.
4. Explain the importance of strong documentation in cyberforensics profession.
5. Is there a difference between “digital forensics” vis-à-vis “computer forensics”? Explain.
6. Explain the role of digital forensics. What do you think is the reaction of traditional legal communities about role of “digital evidence” in crime? Prepare a debate note by considering your own view as well as by talking to the legal community professionals and/or the professors in the institute where you are studying.
7. Explain the importance of “chain of custody” concept. Provide illustrations to support your answer.
8. Do you think the *Indian Evidence Act* is adequate to handle digital evidence? Explain your answer with supporting illustrations.
9. Explain some of the best practices in handling digital evidence. Explain what “rules of evidence” are.
10. Explain how an E-Mail can be traced for forensics purpose. Outline the various key steps involved.
11. What are the various phases and activities involved in the life cycle of a forensics investigation process? Support your answer through various relevant examples.
12. What are the different types of digital analysis that can be performed on the captured forensics evidence?
13. What are the typical elements of a digital forensics investigation report?
14. What would be the nature of evidence collected for network forensics?
15. What role does an “expert witness” play in a cyberforensic/digital forensics case?
16. What precautions should be taken while collecting electronic evidence? What are the things to be avoided during a cyberforensic/digital forensics investigation? Support your answers with examples. What are the things that *cannot* be avoided?
17. Explain why the NDA (non-disclosure agreement) is important in a forensics investigation. What do you think are the risks that may arise if an NDA is not signed before commencing the investigation?
18. Highlight the key steps to be performed in solving a computer forensics case.
19. Explain what is required in setting up a computer forensics laboratory. What tools are required on hardware and software side?
20. What steps do the network hackers execute, as explained in this chapter?
21. What is a “social networking” site? What are the security threats that can emanate from social networking sites?

22. What are “rootkits.” Why are they dangerous? How do rootkits help cyberattackers?
23. What are the major international regulations (the “Big 4 Laws”) as mentioned in this chapter that impact forensics?
24. Explain the “complexity” and “quantity” problems faced in digital forensics investigation.
25. Explain the “data privacy” challenge in cyberforensics. Support your point with suitable illustrative examples.
26. Do you think that using “counter-forensics privacy tools” is a good idea? Why? Explain with examples.
27. Provide an overview of how “data mining” techniques can be applied in cyberforensics.
28. Highlight some of the key differences between an “audit” and a “cyberforensics investigation.”
29. What, do you think, has led to antiforensics behaviors and tools? Elaborate your answer with suitable examples. Explain how the criminals exploit the situations.

REFERENCES

- [1] Following are the links for COFEE:
 - http://en.wikipedia.org/wiki/Computer_Online_Forensic_Evidence_Extractor (6 November 2009).
 - http://www.groundreport.com/Media_and_Tech/Microsoft-Makes-the-COFEE/2860183 (6 November 2009).
 - <http://www.postchronicle.com/cgi-bin/artman/exec/view.cgi?archive=68&num=144908> (6 November 2009).
 - <http://www.wired.com/threatlevel/2008/04/microsoft-gives> (6 November 2009).
 - <http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=1616> (6 November 2009).
 - <http://www.ghacks.net/2008/04/29/computer-online-forensic-evidence-extractor/> (6 November 2009).
- [2] Following are some useful links on *Access Data’s FTK tool kit*:
 - Access Data’s Home Page: <http://www.accessdata.com/> (21 December 2009).
 - Access Data’s products for various types of forensics investigations: <http://www.accessdata.com/Products.html> (21 December 2009).
 - The forensics features of access data’s toolkit: <http://www.accessdata.com/forensictoolkit.html> (21 December 2009).
 - This is about FTK 2.0.2 to 2.1 Upgrade Instructions: http://ftk21.accessdata.com/Upgrade_from_2-02_to_2-1.pdf (21 December 2009).
- [3] Useful links on *Guidance Software’s EnCase* can be visited at:
 - <http://www.digitalintelligence.com/software/guidancesoftware/encase/> (21 December 2009). Following link is about news accolade on this tool:
 - <http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=416497> (22 December 2009). The SC Maganize has announced this tool to be one of the best; a report on that can be seen at:
 - <http://www.scmagazineus.com/guidance-software-encase-forensic-v-6/review/159/> (18 December 2009). To learn about Guidance Software’s EnCase Portable, visit a video demo clip at:
 - <http://vimeo.com/5702414> (10 December 2009). To know more about Guidance Software’s EnCase® Portable having won Cygnus Law Enforcement Group Award in Forensics Category, visit:
 - <http://finance.yahoo.com/news/Guidance-Softwares-EnCase-bw-4161315896.html?x=0> (25 December 2009).
- [4] Following are some useful links on “File Carving” that explains what is “file carving”
 - http://www.fim.uni-linz.ac.at/Lva/IT_Recht_Computerforensik/File_carving.pdf (16 December 2009). A good presentation on the *Advances and Challenges in File Carving* can be read at:

- http://www.korelogic.com/Resources/Projects/dfrws_challenge_2006/DFRWS_2006_File_Carving_Challenge.pdf (3 April 2010). This is a highly technical presentation.
Visit following links that explains about “file carving”:
 - http://en.wikipedia.org/wiki/File_carving (16 December 2009).
A useful note on file carving can be read at:
 - <http://www.file-carving.com/> (22 December 2009).
Read about Foremost’s File Carving/Data Carving Tool at:
 - http://www.secguru.com/link/foremost_file_recovering_data_carving_tool (21 December 2009).
To know about *Scalpel: A Frugal, High Performance File Carver*, refer to:
 - <http://www.digitalforensicsolutions.com/Scalpel/> (24 December 2009).
- [5] To know more on *Sleuth Kit*, visit:
- http://en.wikipedia.org/wiki/The_Sleuth_Kit (23 December 2009).
An excellent technical document on the Sleuth Kit is worth reading at:
 - <http://www.markosworld.com/forensics/cmarko-tskintro.pdf> (17 December 2009).
To know more about the Sleuth Kit Informer, visit:
 - <http://phoenix.calpoly.edu/~kvoelker/cis122/Webpage/current/sleuthkit-informer-2.html> (25 December 2009).
The Sleuth Kit (TSK) demonstration can be accessed in a document at:
 - http://www.denisfrati.it/pdf/TSK_v201_Demonstration.pdf (23 and 24 December 2009).
- [6] For open-source forensics tools-related papers, visit:
- http://www.digital-evidence.org/papers/open-src_legal.pdf (23 December 2009).
 - <http://www.opensourceforensics.org/> (2 April 2010)
 - <http://www.opensourceforensics.org/tools/index.html> (30 March 2010).
- [7] The Pune Newsline Article of 18 December 2009.
- [8] Wireless network forensics resources are available at:
- http://en.wikipedia.org/wiki/Wireless_forensics (25 December 2009).
For a technical article on *802.11 Network Forensic Analysis*, visit the link at:
 - http://www.sans.org/reading_room/whitepapers/wireless/_802_11_network_forensic_analysis_33023 (1 January 2010).
Tools and techniques for network forensics are available at:
 - http://airccse.org/journal/nsa/0409s_2.pdf (11 January 2010).
Network Forensics Solutions paper is available at:
 - <http://net-forensics.blogspot.com/> (11 January 2010).
A compact article on *Network Forensics* can be found at:
 - <http://www.bitcricket.com/downloads/Network%20Forensics.pdf> (11 January 2010).

[9] For STD (a Linux-based security tool), visit: <http://s-t-d.org/> (14 January 2010). It is an STD 0.1 security tools distribution.
For Sleuth Kit, visit:

 - <http://www.sleuthkit.org/> (10 January 2010).
For Portable EnCase Tool, visit:
 - <http://www.guidancesoftware.com/encase-portable.htm> (10 January 2010).

[10] For *Hard Copy Imaging Techniques*, you can visit the following links:
To understand what Rimage Corporation does, visit:

 - <http://www.intellistor.co.za/Rimage.htm> (12 January 2010)
 - http://www.cdmediaworld.com/hardware/cdrom/news/0105/rimage_cd_protection.shtml (12 January 2010).
 To know more on Voom Technologies HardCopy 3 Forensics Hard Drive Imager, visit:

 - <http://www.encodedataproducts.com/Voom-Technologies-HardCopy-III-1-2-Portable-Forensic-Hard-Drive-Duplicator-p-2146.html> (10 January 2010).

- <http://www.cds.com/Rapid-Image-7020CS-with-2-x-3-5-Drive-Caddies-p/fgr-0021-000b.htm> (6 September 2010).
- [11] See the paper *Benchmarking Hard Disk Duplication Performance in Forensic Applications* by Robert Botchek, at:
http://www.tableau.com/pdf/en/Tableau_Forensic_Disk_Perf.pdf (10 January 2010).
- [12] To know more about the equipment called FastBloc, visit:
- <http://www.encase.co.za/solutions/accessories/index.shtm> (It shows the two varieties of FastBloc: one for field use and the other for laboratory use).
The Data Sheet for FastBloc is available at:
 - http://www.forensics.ie/images/products/guidance_fastbloc_datasheet.pdf (11 January 2010).
For Guidance Software's FastBloc Field Edition Write-Blocking Device Forensically Validated by NIST, visit:
 - <http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=252266> (11 January 2010).
The User Manual for Guidance Software FastBloc Field Edition is available at:
 - <http://www.agapeinc.in/FastBlocFEmanualRevC.pdf> (18 Sept 2010).
- [13] Refer to the following links with regard to Box 7.13:
- www.guillermito2.net/stegano/ideas.html (29 October 2009).
 - www.guillermito2.net/stegano/jpegx/index.html (29 October 2009).
 - <http://www.guillermito2.net/index.html> (29 October 2009).
 - www.guillermito2.net/stegano/invisiblerecrets/index.html (29 October 2009).
 - <http://www.guillermito2.net/index.html> (29 October 2009).
 - www.securityfocus.com/tools/1434 (29 October 2009).
 - www.guillermito2.net/stegano/imagehide/index.html (29 October 2009).
- [14] Covert channel analysis discussion can be found at the following site:
- http://www.cs.rice.edu/~dwallach/courses/comp527_s99/covert-channels.pdf (6 September 2009).
- [15] Watermarking FAQs are available at the following links:
- http://www.visualwatermark.com/watermarking_faq.htm (1 November 2009).
 - <http://www.bluespike.com/technology/giovanni/faq/> (1 November 2009).
 - <http://www.watermarkingworld.org/faq.html> (1 November 2009).
 - <http://www.digitalwatermarkingalliance.org/faqs.asp> (1 November 2009).
 - http://dcl.ipc.kuas.edu.tw/digital_watermarking.htm (1 November 2009).
- [16] The three approaches to hiding information are discussed in the paper *Steganalysis: A Steganography Intrusion Detection System* by Angela D. Orebaugh of George Mason University. The paper is available at the following link at: http://www.securityknox.com/Steg_project.pdf (11 January 2010).
- [17] Refer to the excellent 3Com Whitepaper *Understanding IP Networking: Everything You Ever Wanted to Know* (Class A, Class B, Class C and Class D Networks, Subnetting, Classful IP Addressing etc. are all explained) in the following link:
- http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf (14 January 2010).
To understand TCP/IP addressing and Subnetting Basics, visit the link at:
 - <http://support.microsoft.com/kb/164015> (16 January 2010).
There is a video clip about A+ Certification: Understanding TCP/IP at the following link:
 - <http://www.youtube.com/watch?v=friWeGyes6Ew> (12 January 2010).
Another good technical documentation on Introduction to TCP/IP protocol architecture can be found at the following link:
 - <http://cit.wta.swin.edu.au/cit/subjects/CITP0040/docs/tcpip.htm> (9 January 2010).
- [18] Following link lists the social networking sites:
http://en.wikipedia.org/wiki/List_of_social_networking_websites (22 January 2010).

- [19] The case described by Steinhauer. J. (2008) *Verdict in MySpace Suicide Case* is available at the following link:
<http://www.nytimes.com/2008/11/27/us/27myspace.html?ref=todayspaper> (12 December 2009).
- [20] For NIST Guidelines on Security Incident Response Handling, readers can visit the following links where these documents are available: The Special Publication 800-61 of NIST *Computer Security Incident Handling Guide* is available at:
- <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf> (19 February 2010).
- The NIST Special Publication 800-86 *Guide to Integrating Forensic Techniques into Incident Response* is available at:
- http://www.cirosec.de/fileadmin/pdf/veroeffentlichungen/NIST_Booklet.pdf (27 February 2010).
- [21] For *Write Blockers*, visit the following links at <http://www.forensicfocus.com/write-blocker-review-230709> (29 January 2010).
<http://forensicfocus.blogspot.com/2009/07/write-blocker-review.html> (29 January 2010).
<http://blogs.sans.org/computer-forensics/2008/10/01/three-hard-drive-imaging-tools/> (29 January 2010).
- [22] The Paper *Live Forensic Acquisition as Alternative to Traditional Forensic Processes* by Marthie Lessing from Council for Scientific and Industrial Research Meiring Naudé Road, Scientia, Pretoria, South Africa and Basie von Solms from Academy for Information Technology University of Johannesburg, Auckland Park Kingsway Campus, Johannesburg, South Africa is available at:
http://researchspace.csir.co.za/dspace/bitstream/10204/3141/1/Lessing5_2008.pdf (1 March 2010).
- [23] For “Daubert Hearing” and “Daubert Test,” refer to the following links:
- <http://www.helium.com/items/1807122-daubert-hearing-on-expert-and-scientific-evidence> (16 February 2011).
- [24] • <http://www.mobar.org/journal/1997/novdec/beabout.htm> (16 February 2011).
• http://en.wikipedia.org/wiki/Daubert_standard (16 February 2011).
- [24] The article *Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection* by Erin E. Kenneally is available at:
- http://www.lawtechjournal.com/articles/2005/05_051201_Kenneally.php (1 March 2010).
- The article *Techno Security Guide to eDiscovery and Digital Evidence* can be found at:
- <http://www.scribd.com/doc/21581538/Techno-Security-s-Guide-to-E-Discovery-and-Digital-Forensics> (25 February 2010).

The Paper *Automatically Creating Realistic Targets for Digital Forensics Investigation* by Frank Adelstein from ATC-NY, Yun Gao and Golden G. Richard III from Department of Computer Science University of New Orleans, USA is available at:

 - <http://www.cs.uno.edu/~golden/Stuff/falcon2005.pdf> (28 February 2010).

The Paper *Bringing Science to Digital Forensics with Standardized Forensic Corpora* by Simson Garfinkel, Paul Farrell, Vassil Roussov and George Dinolt from Graduate School of Operational and Information Sciences, Department of Computer Science, Naval Postgraduate School, Monterey, CA 93943, USA is available at:

 - <http://www.dfrws.org/2009/proceedings/p2-garfinkel.pdf> (22 February 2010).

The paper *An Open-Source Forensics Platform* by R. Koen and M. S. Olivier is available at:

 - <http://mo.co.za/open/reco.pdf> (12 February 2010).

[25] NIST Special Publication 800-92 *Guide to Computer Security Log Management* is available at:

 - <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf> (1 March 2010).

NIST’s Computer Security Incident Handling Guide can be visited at:

 - <http://www.scribd.com/doc/17921434/nist-sp-800061r1-computer-security-incident-handling-guide-200805>

- [26] The Paper *Building Evidence Graphs for Network Forensics Analysis* by Wei Wang, Thomas E. Daniels from Department of Electrical and Computer Engineering, Iowa State University Ames, Iowa can be downloaded from the following link:
<http://www.acsac.org/2005/papers/125.pdf> (12 January 2010).
- [27] The *Dissertation Supporting the Visualization and Forensic Analysis Of Network Events*, submitted to the Department of Computer Science and the Committee on Graduate Studies of Stanford University in partial fulfillment of the requirements for the degree of Doctor of Philosophy can be downloaded at:
- <http://graphics.stanford.edu/papers/dphantesis/doantam.phan.thesis.pdf> (1 March 2010).
- Details of the *Workshop on Data Mining for Cyber Threat Analysis* in conjunction with IEEE International Conference on Data Mining 9–12 December 2002, Maebashi TERRSA, Maebashi City, Japan can be found at:
- http://www-users.cs.umn.edu/~aleks/icdm02w/workshop_schedule.pdf (24 February 2010).
- The Thesis, *Exploring And Validating Data Mining Algorithms For Use In Data Ascription* by Daniel P. Huynh in June 2008, submitted at the Naval Postgraduate School can be found at:
- http://theses.nps.navy.mil/08Jun_Huynh.pdf (29 March 2010).
- For Abstracts of the Technical Papers (Ontology-Driven Text Mining for Digital Forensics, Apply Data Mining Techniques for Cyber Intrusion Detection, Apply Dynamical Bayesian Network to Query Digital Forensics, Intelligent Environmental Query on Spatial Data, Intelligent Land Planning on Relational Spatial Data), refer to:
- <http://escience.anu.edu.au/project/subject-Others/NICTA07DMProjectTopicsProposals.doc> (4 April 2010).
- [28] Kargupta, H., Liu, K. and Ryan, J. *Privacy-Sensitive Distributed Data Mining from Multi-Party Data*. Proceedings of the 1st NSF/NIJ Symposium on Intelligence and Security Informatics, 2003, LNCS 2665, Springer-Verlag, pp. 336–342.
- [29] Chau, M., Xu, J.J. and Chen, H. *Extracting Meaningful Entities from Police Narrative Reports*. Proceedings of National Conference on Digital Government Research, 2002, Digital Government Research Center, pp. 271–275.
- [30] Hauck, R.V. *et al.* (2002) Using coplink to analyze criminal-justice data, *Computer*, pp. 30–37.
- [31] Senator, T. *et al.* (1995) The FinCEN artificial intelligence system: identifying potential money laundering from reports of large cash transactions, *AI Magazine*, 16 (4), pp. 21–39.
- [32] Lee, W., Stolfo, S.J. and Mok, W. A Data Mining Framework for Building Intrusion Detection Models. Proceedings of 1999 IEEE Symposium on Security and Privacy, 1999, IEEE CS Press, pp. 120–132.
- [33] To understand how “Insider Trading” works, visit:
 - <http://money.howstuffworks.com/insider-trading1.htm> (5 April 2010).
 - <http://beginnersinvest.about.com/cs/newinvestors/a/102702a.htm> (5 April 2010).
 - <http://www.mysmp.com/stocks/insider-trading.html> (5 April 2010).
- [34] Privacy issues discussed in the article *Working from Home: Myths and Truths* by Nina Godbole in PCQuest February 2010 issue posted at:
 - <http://pcquest.ciol.com/content/topstories/2010/110020105.asp> (4 April 2010).The write-up based on the topic *Challenges in Mobile Workforce Mgmt* at the IT SummIT 2009 at the Cyber Media event is available at:
 - <http://pcquest.ciol.com/content/techtrends/2010/110010806.asp> (4 April 2010).
- [35] A table showing feature comparison of the antiforensics privacy products mentioned in Section 7.19 (Antiforensics) is available at: <http://www.privacy-software-review.toptenreviews.com/> (2 April 2010).
- [36] The tool “timestomp” is available at: www.metasploit.com/projects/antiforensics/ (1 April 2010).

See the presentation *Metasploit Antiforensic Project* available at:

http://www.metasploit.com/data/antiforensics/ToorCon7-Metasploit_AntiForensics.ppt
(8 April 2010).

- [37] Additional Information about “Slacker” can be accessed at:

- <http://www.forensickb.com/2007/10/enscript-to-detect-use-of-slackeree.html>

(9 April 2010). Here it is explained how ‘Enscript’ detected the use of “slacker.exe”. To know more on “slacker.exe,” visit the following site:

- <http://www.forensicswiki.org/wiki/Slacker>
(9 April 2010)

FURTHER READING

Additional Useful Web References

1. On the International Association of Crime Analysts Page in the following link, there is a complete table containing the listing of Crime Analysis Software:
<http://www.iaca.net/Software.asp> (27 February 2010).
2. To understand the meaning of “end-to-end digital forensics,” the following sites can be visited:
 - For Digital Forensics Research Workshop, visit: www.dfrws.org (31 May 2009).
 - For International Journal of Digital Evidence, visit: www.ijde.org (31 May 2009).
3. For *Forensic File Formats*, refer to: http://www.forensicswiki.org/index.php?title=Forensic_file_formats (6 June 2009).
4. There is a basic article for non-technical readers to understand what “Rootkits” are and how to remove them. To know more on this, visit:
 - <http://www.virus.gr/portal/en/content/rootkits-what-are-they-how-remove-them> (8 April 2010).
 A technical paper on *database rootkits* (2005) by Alexander Kornbrust is available at:
 - http://www.red-database-security.com/wp/db_rootkits_us.pdf (8 April 2010).
 Oracle Rootkits are discussed in a paper available at:
 - http://www.red-database-security.com/wp/oracle_rootkits_2.0.pdf (8 April 2010).
 A technical presentation on “*In Memory Rootkits*” is available at:
 - <http://www.databasesecurity.com/oracle-backdoors.ppt> (8 April 2010).

To have an overview of *Unix Rootkits Overview and Defense* by Anton Chuvakin, visit:

- www.rootsecure.net/content/downloads/pdf/unix_rootkits_overview.pdf (8 April 2010).
- Microsoft BlueHat Security Briefings: Spring 2006 Sessions and Interviews are available at:
 - <http://www.microsoft.com/technet/security/bluehat/sessions/default.mspx> (11 April 2010).
- 5. Some *free downloadable File Splitting software utilities* can be accessed at readers’ own risk by visiting:
 - <http://www.snapfiles.com/Freeware/downloader/fwfilesplit.html> (3 June 2009).
- 6. The home page of the *Australian Institute of Criminology* can be visited at:
 - <http://www.aic.gov.au/> (23 April 2009).
- 7. Those aspiring to pick up a course in cyberforensics with adequate hands-on content, may visit:
 - <http://blogs.thehindu.com/delhi/?p=20694> (23 October 2009).
- 8. For *Digital Forensic/Computer Forensic/Cyber Forensic Frequently Asked Questions* (FAQs), visit:
 - Computer forensics FAQs at:
 - <http://www.evestigate.com/Computer%20Forensics%20FAQ.htm> (24 October 2009).
 - Forensics examination FAQs at:
 - <http://www.patctech.com/faq/forensic.shtml> (24 October 2009).
 - Digital detective FAQs at:
 - <http://www.digital-detective.co.uk/faq.asp> (24 October 2009).

Computer forensics FAQs at:

- http://www.newyorkcomputerforensics.com/learn/forensics_faq.php (24 October 2009).
- <http://www.ccl-forensics.com/237/FAQ.html> (24 October 2009).
- <http://www.evidencetalks.com/faq.html> (24 October 2009).

Computer forensics basics FAQs at:

- <http://www.computerforensicsworld.com/modules.php?name=News&file=article&sid=1> (24 October 2009).
- <http://www.setecinvestigations.com/resources/faqs.php> (24 October 2009).

Computing hacking forensics FAQs at:

- <http://www.cfila.com/forensicsfaq.htm> (24 October 2009).

9. For those interested in seeking a digital forensics career, the following list of links may be useful: FAQs about digital forensics program, visit the following sites at:

- <http://forensics.cs.uri.edu/faq.php> (26 October 2009).
- http://www.forensiccareers.com/index.php?option=com_content&task=view&id=23&Itemid=26 (26 October 2009).
- <http://computerforensics911.com/> (26 October 2009).

FAQs to Digital Forensics Certification Board, visit:

- <http://www.ncfs.org/dfcb/faqs.html> (26 October 2009).

10. For covert channels, visit:

- http://en.wikipedia.org/wiki/Covert_channels (1 November 2009).

To know more about covert channels and steganography discussion, visit:

- <http://www.covertchannels.org/> (1 November 2009).

11. For *Information Hiding: Steganography & Digital Watermarking*, refer to:

- <http://www.jjtc.com/Steganography/> (1 November 2009).

12. For *Understanding Digital Steganography*, refer to:

- <http://fanaticmedia.com/infosecurity/archive/Sep09/Digital%20Steganography.htm> (30 October 2009).

All about steganography is explained at:

- <http://palisade.plynt.com/issues/2005Apr/steganography/> (1 November 2009).

13. For those readers who are highly technical minded can refer to:

<http://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-smith.pdf> (13 January 2010). It is about forensics lessons learned by a person working with the Department of Defense.

14. For *California SB (Security Breach) 1386*, refer to: For the SB 1386 Compliance Management Toolkit, visit:

- <http://www.sb-1386.com/> (20 February 2010). For SB 1386, refer to:
- http://en.wikipedia.org/wiki/SB_1386 (20 February 2010). For SB-1386 Introduction, refer to:
- <http://www.sb-1386.com/sb-intro.htm> (20 February 2010).

15. Some more links to California's new mandatory disclosure law are as follows:

- http://searchsecurity.techtarget.com/tip/1,289483,sid14_gc1901999,00.html (19 February 2010).
- http://www.privacyrights.org/ar/Security_Breach.htm (19 February 2010).
- <http://www.bitpipe.com/tlist/California-Senate-Bill-1386.html> (19 February 2010).
- <http://library.findlaw.com/2003/Sep/30/133060.html> (19 February 2010).

16. There is an informative document *What Judges Should Know About Computer Forensics* available at:

http://www.craigball.com/What_Judges_Computer_Forensics-200807.pdf (1 February 2010).

17. An interesting article *Sending email: Can you be arrested?* is available at:

<http://specials.rediff.com/money/2008/jul/29cyber.htm> (20 February 2010).

18. The article *Chinese Hackers and India Cyber Forensics* can be visited at:

<http://www.thedarkvisitor.com/2008/08/chinese-hackers-and-india-cyber-forensics/> (1 March 2010).

19. Following link explains what Facebook is for:
<http://www.youtube.com/watch?v=kFKHaFJzUb4&NR=1> (1 March 2010).
20. *Incident Management in the Age of Compliance* is the article that addresses the basics of doing what the laws tell you to do (FISMA, HIPAA, PCI-DSS) at:
http://www.computerworld.com/s/article/9019559/Incident_management_in_the_age_of_compliance?taxonomyName=Disaster_Recovery (21 February 2010).
21. Useful blogs on computer investigation is found at:
http://forensic.to/links/pages/Forensic_Sciences/Field_of_expertise/Computer_Investigation/ (14 February 2010).
22. C-DAC releases five new products at Elitex 2008, visit:
 - <http://enterthegrid.com/primeur/08/articles/weekly/AE-PR-02-08-61.html> (6 September 2010).
 One of the products is *Cyber Investigation and Analysis Tools for Network Forensics* and the Frequently Asked Questions document *Intrusion Detection FAQ: Can you explain traffic analysis and anomaly detection?* is available at:
 - http://www.sans.org/security-resources/idfaq/anomaly_detection.php (1 March 2010).
23. For the Global News on Forensics Computing, visit:
<http://www.f3.org.uk/modules/news/index.php?storytopic=2&start=95> (5 February 2010).
24. *How Forensics works* is very well explained at:
<http://computer.howstuffworks.com/computer-forensic3.htm> (9 April 2010).
25. DoD List of Cyber Forensics Tools can be obtained by visiting the link at:
<http://www.dc3.mil/dcci/dcciCyberFiles.php> (9 September 2010).
26. Some free file recovery methods are as follows:
<http://pcsupport.about.com/od/filerecovery/tp/free-file-recovery-programs.htm> (18 September 2010).
 To learn about some of the Recognized Data Overwriting Standards, visit:
http://www.dataerasure.com/recognized_overwriting_standards.htm (18 September 2010).

These methods of data sanitization ensure regulatory compliance.

27. The Paper *Open Source Digital Forensics Tools: The Legal Argument* by Brian Carrier is available at:
http://www.digital-evidence.org/papers/opensrc_legal.pdf (25 February 2010).

Books

1. Volonino, L. and Anzaldua, R. (2008) *Computer Forensics for Dummies*, Wiley Publishing.
2. Casey, E. (ed.) (2002) *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press, CA.
3. Marjie, B.T. (2003) *Computer Forensics and Cyber Crime: An Introduction*, Prentice Hall.
4. Anthony, R. (2007) *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*, Syngress.
5. McKenzie, M.A. (2009) *Digital Forensics: Digital Evidence in Criminal Investigations*, Wiley.
6. Johnson, T.A. (ed.) (2006) *Forensic Computer Crime Investigation*, CRC Press, Boca Raton, FL.
7. Casey, E. (ed.) (2004) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 2nd edn, Academic Press.
8. Sood, V. (2010) Leading electronic evidence in the court: critical analysis and the stepwise process, *Cyber Crimes, Electronic Evidence & Investigation: Legal Issues*, 1st edn, NABHI Publication, New Delhi, p. 177.
9. Marcella, A.J., Jr. and Menendez, D. (2008) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crime*, 2nd edn, Auerbach Publications.
10. Steve, B. (2007) *EnCase Computer Forensics: The Official EnCE – EnCase Certified Examiner Study Guide*, 2nd edn, John Wiley & Sons.
11. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India. Readers can refer to Chapters 11 and 12 and the entire Part III of this book; it is dedicated to logical and network security-related topics. E-Mail security is also discussed in that part of the book. The OSI 7 Layer Model is also explained.
12. ibid – Chapter 2 (Threats to Information Systems).

13. Ibid – Chapter 4 (Information Security Management in Organizations).
14. Ibid – Chapter 5 (Building Blocks of Information Security)
15. Ibid – Chapter 12, Section 12.5 (The OSI Seven-Layer Model) and Section 12.7 (Network Protocols). See p. 210 about Tunneling Protocols.
16. Ibid – Chapter 13 (Cryptography and Encryption).
17. Ibid – Chapter 14 (Intrusion Detection for Securing the Networks).
18. Ibid – Chapter 17 (Security of Wireless Networks).
19. Ibid – Chapter 35, Section 35.9 explains Penetration Testing and Vulnerability Scanning and the difference between the two, etc.
20. EC-Council (2009), *Computer Forensics: Investigating Wireless Networks and Devices*, EC Council Press, New York, USA.
21. Volonino, L and Anzaldua, R. (2008) Computer Forensics for Dummies (For Dummies (Computer/Tech))John Wiley & Sons Ltd., USA
22. Caloyannides, M.A. (2001) *Computer Forensics and Privacy*, Artech House (Artech House Computer Security Series), Boston, MA.
23. Caloyannides, M.A. *Privacy Protection and Computer Forensics*, 2nd edn, Artech House (Artech House Computer Security Series), Boston, MA.
24. To know more on data mining, refer to the following books:
Han, J., Kamber, M. and Pei, J. (2005) *Data Mining: Concepts and Techniques*, 2nd edn, The Morgan Kaufmann Series in Data Management Systems, Morgan Kaufmann Publishers.
Cios, K.J., Pedrycz, W., Swiniarski, R.W. and Kurgan, A.K. (2007) *Data Mining: A Knowledge Discovery Approach*, Springer.
Shmueli, G., Patel, N.R. and Bruce, P.C. (2006) *Data Mining for Business Intelligence: Concepts, Techniques, and Applications in Microsoft Office Excel with XLMiner*, Wiley.
Thuraisingham, B.M. *Data Mining: Technologies, Techniques, Tools, and Trends*, CRC Press.
25. Microsoft Word version of *FastBloc User Guide Manual* can be downloaded from the following link: http://www.agapeinc.in/FastBloc-IDE_manual.doc (10 September 2010).

Articles and Research Papers

1. A 2008 presentation by Bruce Nikkel titled *Practical Computer Forensics using Open Source Tools* is available at: http://www.ch-open.ch/events/slides/2008/080612_nikkel08.pdf (9 April 2010).
2. *Computer Forensics*, 56 (1), January 2008 issue is available at: http://www.justice.gov/usaio/eousa/foia_reading_room/usab5601.pdf (12 February 2010).
3. Borck, J. (2001) *Leave the cybersleuthing to the experts* – refer to this article in the following URL: <http://www.infoworld.com/articles/tc/xml/01/04/09/010409tccounter.html> (22 December 2005).
4. Bitpipe (2005) *Computer Forensics*. This article is available at: <http://www.bitpipe.com/tlist/Computer-Forensics.html> (27 December 2005).
5. Burdach, M. (2005) *Digital Forensics of the Physical Memory* is available at: http://forensic.seccure.net/pdf/mburdach_digital_forensics_of_physical_memory.pdf (21 June 2005).
6. A paper by Liu, Q., Sung, A.H. and Qiao, M. *Detecting Information-Hiding in WAV Audios*, Computer Science Department and Institute for Complex Additive Systems Analysis, New Mexico Tech. can be accessed at:
 - <http://figment.cse.usf.edu/~sfefilat/data/papers/TuBCT9.47.pdf> (7 May 2009).Harrill, D.C. and Mislan, R.P. (2007) A small scale digital device forensics ontology, *Small Scale Digital Device Forensics Journal*, 1 (1). The paper is available at:
 - http://www.ssddfj.org/papers/SSDDFJ_V1_1_Harrill_Mislan.pdf (1 September 2009).
7. Brinson Ashley, Robinson Abigail, Rogers Marcus (2006) A cyber forensics ontology: Creating a new approach to studying cyber forensics, *Digital Investigation* 3S, S37–S43 can

- be accessed at: <http://www.dfrws.org/2006/proceedings/5-Brinson.pdf> (6 September 2010).
8. Marsico, C.V. and Rogers, M.K., iPod Forensics, The CERIAS Tech Report 2005-13, the Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086. The paper can be accessed at:
https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-13.pdf (2 August 2009).
 9. Marsico, C.V. Digital Music Device Forensics, CERIAS Tech Report 2005-27, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086. It is a Thesis Submitted to the Faculty of Purdue University and is available at:
https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-27.pdf (31 August 2009).
 10. Some links iPod Forensics are as follows:
https://www.cerias.purdue.edu/apps/reports_c (2 September 2009).
<http://www.cerias.purdue.edu/search/site.php?q=forensics> (2 September 2009).
 11. The following site lists the forensics vendors – the software and hardware tools are alphabetically listed, visit: <http://www.e-evidence.info/vendors.html> (12 September 2009).
 12. For an interesting paper whether Computer Forensics is based on Computer Science or Forensics Science, visit: http://www.ics.heacademy.ac.uk/events/presentations/736_HEA-ICS-TchCompFor_paper.pdf (12 September 2009).
 13. For Cisco Router Forensics, the following link can be accessed at:
<http://www.forensics.nl/presentations> (23 September 2009).
This is an excellent reference for lawyers practicing in cybercrime cases and working with digital forensics experts, here is the link where some excellent technical articles are available. They explain many technical aspects such as – difference between “clone” and “image” of drive, how do you make a “forensically-sound” duplicate of a drive. How can you prove the duplicate drive is forensically sound. Examining and analyzing E-Mail headers for forensics analysis and how to look for a good forensics expert, etc. is also covered in this set of articles.
 14. Van Horenbeeck, M. *Deception on the network*, School of Computer and Information Science at Edith Cowan University. Malicious use of covert channels is explained in this paper. This paper can be accessed at: http://www.daemon.be/maarten/Vanhorenbeeck_covertchannels.pdf (31 October 2009).
 15. A 2006 student technical report on covert channel research is available at:
<http://staff.science.uva.nl/~delaat/snb-2005-2006/p27/report.pdf> (25 October 2009). It is the Research Report for RP1 based on student work by Marc Smeets and Matthijs Koot as part of their work in the course MSc in System and Network Engineering at the University of Amsterdam
 16. There is a paper that explains a covert communication channel that exists in virtually all forms of packet switching data networks. It is a paper by Bo Yuan and Peter Lutz, Department of Networking, Security, and Systems Administration, Golisano College of Computing and Information Sciences at the Rochester Institute of Technology, New York 14623. Visit http://www.ist.rit.edu/~byuan/papers/boyuan_peterlutz05.pdf (25 October 2009).
 17. Chauhan, S. (2005) *Analysis and Detection of Covert Network Channels*, Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County. The paper is available at: <http://www.cisa.umbc.edu/courses/cmsc444/fall05/studentprojects/sweetly.pdf> (1 November 2009).
 18. Uma Devi G. (2006) *Steganography-Survey on File Systems*, as part of MS by Research – CSE, IIIT (Indian Institute of Information Technology), Hyderabad. The paper can be accessed at:
<http://researchweb.iiit.ac.in/~umadevi/steg.pdf> (1 November 2009).
 19. Gulati, K. (2003) A Dissertation on *Information Hiding Using Fractal Encoding*,

- submitted in partial fulfillment of the requirements for the degree of Master of Technology at the IIT, Bombay. It is under the guidance of Prof. Vikram M. Gadre at the School of Information Technology at the IIT, Mumbai. It is accessible at:
<http://www.it.iitb.ac.in/~kamal/fractal.pdf> (30 October 2009).
20. Llamas, D., Allison, C. and Miller, A. *Covert Channels in Internet Protocols: A Survey* by, the School of Computer Science at the University of St Andrews, St Andrews KY16 9SX, Scotland, UK. The paper is available at:
<http://gray-world.net/papers/0506-PGNET-Paper.pdf> (1 November 2009).
21. Pan, L. and Batten, L.M. *Reproducibility of Digital Evidence in Forensic Investigations*, School of Information Technology, Deakin University, Australia. The paper is available at:
http://www.dfrws.org/2005/proceedings/pan_reproducibility.pdf (19 December 2009).
22. Ahmed, I. *Steganalysis in Computer Forensics*, School of Computer and Information Science, Edith Cowan University. The paper is available at: http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/10_Ibrahim%20-%20Steganalysis%20in%20Computer%20Forensics.pdf (6 June 2009).
23. Karp, S. (2007) *Facebook's Vulnerabilities*, refer to the following link: <http://publishing2.com/2007/10/31/facebookvulnerabilities/> (10 December 2009).
24. Kessler, G.C. and Schirling, M. (2002) *Computer Forensics: The Issues and Current Books in the Field*. The paper can be found at: http://www.garykessler.net/library/computer_forensics_books.html (26 February 2010).
25. Olsson, J. *Computer Forensics Digital Evidence with Emphasis on Time*. The paper can be accessed at: [http://www.bth.se/tek/aps/mbo.nsf/bilagor/Digital_Evidence_with_EmpHASIS_on_Time_pdf/\\$file/Digital_Evidence_with_EmpHASIS_on_Time.pdf](http://www.bth.se/tek/aps/mbo.nsf/bilagor/Digital_Evidence_with_EmpHASIS_on_Time_pdf/$file/Digital_Evidence_with_EmpHASIS_on_Time.pdf) (2 March 2010).
26. Symon, C. (2009) *Enhanced Event Time-Lining for Digital Forensic Systems*. The paper is submitted in partial fulfillment of the requirements of Edinburgh Napier University for the Degree of Computer Networks & Distributed Systems (Hons), School of Computing. It is available at:
<http://www.dcs.napier.ac.uk/~bill/colin01.pdf> (10 January 2010).
27. Ha, D., Upadhyaya, S., Ngo, H., Pramanik, S., Chinchan, R. and Mathew, S. *Insider Threat Analysis Using Information-Centric Modeling*. The paper can be visited at: <http://www.cse.buffalo.edu/~shambhu/documents/pdf/ifip-chapter-2007.pdf> (2 March 2010).
28. Regan, J.E. (2009) *The Forensic Potential of Flash Memory*. The paper is submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis can be read at: http://simson.net/clips/students/09Sep_Regan.pdf (8 April 2010).
29. There is CIO magazine article, *How Online Criminals Make Themselves Tough to Find, Near Impossible to Nab*. The article can be accessed at:
- <http://www.proofspace.com/UserFiles/File/How%20Anti%20Forensics%20Tools%20Make%20Themselves%20Tough%20to%20Find%20Near%20Impossible%20to%20Nab%20CIO%20com%202007-05-31.pdf>. (10 April 2010).
In this article it is explained how antiforensics tools reveal vulnerabilities in computer forensics tools. An argument is made that the rise of antiforensics tools will force computer investigators to change.
EnCase and Sleuth Kit vulnerabilities are described in a technical paper at:
- https://www.iseccpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf (7 April 2010).
In this 2007 paper titled *Breaking Forensics Software: Weaknesses in Critical Evidence Collection*. Classes of attacks against forensics software are also described in this paper. Pg. 5 of this paper describes sleuth kit weaknesses and Pg. 9 describe EnCase weakness.

30. There is an interesting article *Catch Me if You Can* at the following link: <http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf> (8 April 2010).
31. Kessler, G.C. *Anti-Forensics and the Digital Investigator*, Champlain College, Burlington, VT, USA. The paper can be accessed at: http://igneous.scis.ecu.edu.au/proceedings/2007/forensics/01_Kessler_Anti-Forensics.pdf (10 April 2010).
32. Swanson, I. and Williams, P.A.H. *Virtual Environments Support Insider Security Violations*, SECAU Security Research Centre, Edith Cowan University. The paper is available at: http://scissec.scis.ecu.edu.au/conference_proceedings/2008/forensics/Swanson%20Williams%20Virtual%20environments%20.pdf (9 April 2010).
33. ACPO's Official Release version on *Good Practice Guide for Computer-Based Electronic Evidence* is available at: <http://www.asianlaws.org/library/cci/acpo-guidelines-computer-evidence.pdf> (10 September 2010).
34. Read article *Advanced Forensic Format: An Open, Extensible Format for Disk Imaging* by Garnkel, S., Malan, D., Dubec, K., Stevens, C. and Pham, C. at: <http://www.cs.harvard.edu/malan/publications/aff.pdf> (16 December 2010).

Video Clips

Following links present short clips on various topics discussed in this chapter (digital forensics and perils of posting your information on social networking sites, rootkits, etc.)

1. A basic video presentation explaining *What is Computer Forensic* is available at: <http://www.youtube.com/watch?v=yfigCH7CcFk&feature=related> (7 April 2010).
2. Video clips on *Disk Encryption and other Forensics aspects* are available at:
 - <http://www.privacylover.com/computer-forensics/video-using-eraser-to-delete-files-for-good/> (27 February 2010).
 This is a video for beginners – some introduction on why you should use a secure data wiper

to delete files in your computer. In this video clip, a computer user shows you on screen how to use eraser to safely wipe documents and making them vanish for good.

- <http://www.youtube.com/watch?v=9JoX4uxES7Q&feature=related> (27 February 2010). Here, a forensics expert explains how to seize the evidence.
- <http://www.youtube.com/watch?v=grjIOaE4-aA&feature=related> (27 February 2010). This clip explains what computer forensics experts can do to uncover data and online activity.
- <http://www.privacylover.com/computer-forensics/interview-with-a-computer-forensics-expert/> (27 February 2010). This clip is an interview with a computer forensics expert.
- <http://www.youtube.com/watch?v=hSvswzSy3oA&feature=related> (27 February 2010). This is about computer forensics – this video shows how to trace an E-Mail (Hotmail).
- <http://www.privacylover.com/encryption/video-crash-course-in-full-disk-encryption/> (27 February 2010).

This video is a talk held in December 2008 at the 25th Chaos Communication Congress, under the title *Nothing to Hide*. It is a crash course in full-disk encryption concepts, products and implementation aspects. An overview of both commercial and open-source offerings for Windows, Linux and MacOS X is provided. A programmer's look at the open-source solutions concludes the presentation.

- <http://www.privacylover.com/encryption/review-full-disk-encryption-diskcryptor-v0-7-435-90/> (27 February 2010). This is review of DiskCryptor based on its testing done.
- <http://www.privacylover.com/encryption/review-drivecrypt-plus-pack-full-disk-encryption/> (27 February 2010). This clip is review of Drivecrypt Plus Pack v3.95, full-disk encryption.
- <http://www.privacylover.com/computer-forensics/video-computer-forensic-investigation/> (27 February 2010). At this link, a computer forensics professional explains the basics of

computer forensics, how data is recovered from people's computers and what challenges they face.

- <http://www.privacylover.com/computer-forensics/metasploit-anti-forensic-investigation-arsenal-mafia/> (27 February 2010). This clip is about Metasploit Anti-Forensic Investigation Arsenal (MAFIA).
 - <http://www.youtube.com/watch?v=0HeVx5fkwSY&feature=related> (27 February 2010). Here, an expert explains how website traffic myths are uncovered.
 - <http://www.youtube.com/watch?v=O4ce74q2zqM&NR=1> (27 February 2010). There is a Demo of EnCase Computer Forensics Tool available in this link.
 - <http://www.youtube.com/watch?v=kK6Wd7HVyVM&feature=related> (27 February 2010). This video clip shows basic keyword searching with forensics Tool EnCase.
3. Video clips on *Perils of Social Networking Sites* are available at:
- <http://www.youtube.com/watch?v=ZmQT3SMxATQ&feature=related> (27 February 2010). This clip explains the perils of posting your personal information on social networking sites.
 - <http://www.youtube.com/watch?v=0AtsNyXFg7Y&feature=fvw> (27 February 2010). It explains about dangers of social networking,
 - <http://www.youtube.com/watch?v=azIW1xjSTCo&feature=related> (27 February 2010). This is about how social networks such as Facebook and MySpace impacts private life.
 - 4. A video clip explaining "BIOS Rootkits" is available at: http://www.youtube.com/watch?v=G26oZtzluAQ&feature=player_embedded (10 April 2010).
 - 5. A video clip on antiforensics can be viewed at: <http://pursuitmag.com/anti-computer-forensics/> (9 April 2010)
 - 6. Fourth Amendment Project video clip can be accessed at: http://www.youtube.com/watch?v=mdT_k6Yj_w8 (7 September 2010).

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, D, F, G, I, N, O, Q. These are provided in the companion CD.

8

Forensics of Hand-Held Devices

Learning Objectives

After reading this chapter, you will able to:

- Learn about different types of hand-held devices.
- Get an overview of cell phone characteristics.
- Understand the guidelines for cell phones forensics.
- Understand the forensics aspects of iPhone, iPod and the BlackBerry device.
- Get an overview of forensics of printers, scanners and digital cameras.
- Get an overview of tools used for the forensics of hand-held devices.
- Learn about legal aspects involved in forensics.
- Understand the challenges for law authorities.

8.1 Introduction

In Chapter 7, we learned about the fundamental concepts in computer forensics/digital forensics. We also learned about the role of forensics analysis in cybercrime investigation. The phases involved in a cyberforensics investigation were also described there. We present a brief definition here.



“Computer forensics” is the application of forensic science techniques to the systematic discovery, collection and analysis of digital evidence. It is the preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis using well-defined methodologies and procedures.

The methodology used is acquiring the evidence without altering or damaging (safe custody of the evidence) the original digital evidence, authenticating that the recovered evidence is the same as the original seized and analyzing the data without modifying it (chain of custody concept). The legal aspects of forensics are also explained in Chapter 7. They are relevant here too because we will be introducing some more legal aspects of forensics in this chapter.

With the background of the basic concepts covered in Chapter 7, we will address in this chapter, the forensics of small hand-held devices – mobile phones, iPhones, Smartphones, music and video players such as the iPods, etc. (see Fig. 8.1). Given the popularity of various types of mobile hand-held devices,



Figure 8.1 | Hand-held devices. (a) iPhone; (b) iPod; (c) palm pilot; (d) digital diary; (e) Smartphones; (f) 2 GB MP2 player; (g) portable printer; (h) handycam and (i) PDA.
Source: <http://www.google.co.in>

a dedicated discussion to their forensics is crucial. In fact, “device forensics/hand-held forensics” has emerged as a specialized application of digital forensics. This can be well understood given the rise in workforce mobility and the spread of mobile computing. Such trends have resulted in proliferation of hand-held devices. Chapter 3 (Cybercrime: Mobile and Wireless Devices) also serves as the additional background for this chapter. Refer to links we have provided for leading products that are used in hand-held forensics.^[1]



The terms “device forensics” and “hand-held forensics” are used interchangeably in this chapter.

Before moving to the core part of the chapter, let us understand the working characteristics of cell phones as they are the most familiar hand-held devices. There are security and privacy risks associated with the rising use of mobile handsets! There is no such thing “as just a mobile phone” anymore. Some devices have Bluetooth, which means there is network connectivity. There is a lot more E-Mail and web functionality getting added to mobile phones. Anything stored on that device is business property and needs protection! Several thousand employees use BlackBerrys which are supposed to be more secure than some other phones in the market because they were designed with security in mind. However, employees may try out other phones and some of them are a lot tougher to manage from a security standpoint (e.g., the newly unveiled Apple iPhone).



According to the Internet and Mobile Association of India, Internet usage in the country has risen by 20% in the last year alone with people progressively spending more time online. Indians are increasingly accessing and transmitting sensitive information from their workstations/PCs, from home and while in transit through their laptops, netbooks or Smartphones. India's surge in malicious activity in 2008 moved the country from 11th position for overall malicious activity to 5th in 2009.

8.2 Understanding Cell Phone Working Characteristics

In modern times, cellular mobile phones have become an integral part of communication around the world. Forensics and digital analysis of mobile phones, therefore, is an area of interest, as crimes involving mobile devices are becoming increasingly common in the community. The additional complexity comes from the ability of modern mobile phones to store reasonably large amounts of information. This feature makes them a very attractive target for criminals. It is no wonder then that forensic analysis of mobile phones is gathering momentum all over the world. The following should, however, be noted.



While mobile phones outsell personal computers (PCs) three to one, mobile phone forensics still lags behind computer forensics.

Now let us have an overview of the hardware and software capabilities of cell phones and their associated cellular networks. The overview provides a summary of general characteristics and, where useful, focuses on key features. Developing an understanding of the components and organization of cell phones (e.g., memory organization and use) is a prerequisite to understanding the criticalities involved when dealing with them forensically. For example, cell phone memory that contains user data may be volatile (i.e., random access memory, RAM) and require continuous power to maintain the content, unlike the requirement for a PC's hard disk. Similarly, features of cellular networks are an important aspect of cell phone forensics, since logs of usage and other data are maintained therein.

Hand-held device technologies and cellular networks are rapidly changing, with new technologies, products and features being introduced regularly. Due to the evolution of cellular device technologies, we present only a snapshot of the cell phone area at the present time. Technology evolves continuously and becomes obsolete rapidly. Some products/tools/technologies may become obsolete by the time the book is released. The tools mentioned in this chapter are to the best of our knowledge and as available at the time of writing the book.

8.2.1 Understanding the Types of Cellular Networks

There are different types of digital cellular networks – see Box 8.1. These networks exist due to the distinct and incompatible sets of network protocol standards. The two most dominant types of digital cellular networks are:

1. Code Division Multiple Access (CDMA).
2. Global System for Mobile Communications (GSM) network.

There are other common cellular networks; they include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN). iDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols.

Box 8.1 CDMA, TDMA, GSM, AMPS and DoCoMo and Other Standards

AMPS (Analog)

Analog Mobile Phone Service (AMPS) is sometimes also known as "Advanced Mobile Phone System." Throughout 1980s, the AMPS standard was very prevalent in analog mobile phones. AMPS, however, was not the very first mobile phone standard and therefore the term "Advanced" in the name. Even today, AMPS is still in use – it used for certain high-reliability voice applications – such applications include GM's On*Star service and certain very-low-bandwidth industrial data applications. AMPS phones cannot do text or picture messaging although there is a data element to AMPS used for sending the date, time of day and other low-bandwidth data to mobile phones.

TDMA

Time Division Multiple Access (TDMA) is a digital standard that allows each cellular "channel" to get divided into time slots. This way, TDMA provides a capacity gain over AMPS. With the higher capacity per cell tower and the fact that TDMA is a digital standard, TDMA became a good choice for the replacement of AMPS. As of now, there is high usage of TDMA in the US as well as in few other parts of the world - however, use of TDMA is said to be getting phased out in favor of GSM and CDMA.

TDMA also refers specifically to the standard that is covered by IS-136, which defines a specific type of cellular network. The term TDMA can be used for referring to both a general technique or a specific type of cellular network and this can lead to confusion. Although GSM uses a TDMA air interface, like iDEN does, neither of those systems (i.e., GSM iDEN) is compatible with so-called TDMA cellular networks that follow IS-136.

GSM

Global System for Mobile (GSM) standard is the most widely used world standard for mobile communication. The largest deployment of GSM is in Europe. GSM, as a digital standard, is internally based on TDMA techniques. There are now newer GSM phones that also support digital transmission through General Packet Radio Service (GPRS). GPRS allows sending and receiving of data packets at moderate rates. This extension of GPRS allows new features such as MMS and WAP/web browsing capability. There has been quite some time since the GSM standard has been around. Popularity of GSM continues to grow - due to the addition of GPRS and integration of multiple devices (such as cameras, MP3 players and other gadgets) into GSM phones. Along with these additions, this relatively old standard is actually being phased out within the US.

The GSM cellular system was designed in Europe and today it is used worldwide primarily by Ericsson and Nokia. In the US, nationwide networks are operated by Cingular and T-Mobile. TDMA air interface is used by GSM. TDMA refers to a digital link technology that allows multiple phones to turn by turn share a single carrier, radio frequency channel. In this round robin method of sharing, the channel is used exclusively for a fixed time slice that is allocated. After the allocated time slice, the channel is released waiting briefly while other phones use it. GPRS is the packet-switching enhancement to GSM wireless networks. It was standardized to improve the data transmission. "3G" is the next generation of GSM – it is also known as Universal Mobile Telecommunications System (UMTS). 3G involves enhancing GSM networks with a Wideband CDMA (W-CDMA) air interface.

Box 8.1 CDMA, TDMA, . . . (Continued)

CDMA

Code Division Multiple Access (CDMA) was designed by Qualcomm in the US. It employs spread spectrum communications for the radiolink. When compared to AMPS, TDMA and GSM, CDMA is the newest standard. CDMA allows the highest capacity and highest mobile data throughput. With CDMA, theoretically, the channel capacity you get is several times than that provided by the TDMA. Call Drop is a common phenomenon when cell boundaries are crossed. People who promote CDMA also claim that with CDMA, there are fewer call drops. The CDMA has become very popular in the US, South America and certain parts of Asia – this popularity is said to be due to the newness of CDMA and also because there are other extended standards such as cdma2000 and W-CDMA,. Unlike many other network air interfaces that share a channel, CDMA works differently; it spreads the digitized data over the entire bandwidth available. This way, CDMA is able to distinguish multiple calls by assigning unique sequence code to those calls. In the US, there are successive versions of the IS-95 standard to define CDMA conventions. This is the reason why the term CDMA is often used to refer to IS-95 compliant cellular networks. IS-95 CDMA systems are sometimes referred to as cdmaOne. Evolutionary step for CDMA is cdma2000, TIA/EIA/IS-2000 Series1 and Release A, based on the ITU IMT-2000 standard. In the US, both Verizon and Sprint operate nationwide CDMA networks.

NTT DoCoMo

The expansion of "NTT" is Nippon Telegraph and Telephone and "DoCoMo" is the acronym for "Do Communication Over the Mobile Network." The Japanese word "dokomo," meaning "everywhere", is also cleverly used in this acronym. In Japan, DoCoMo is the most prominent wireless telecommunications operator. DoCoMo is said to have an established base of 50 million subscribers. NTT DoCoMo is another standard worth mentioning. It is from Japanese communications corporation. They introduced a line of cell phone sets containing the equivalent of a digital smart card. These phone sets can contain large amount of data such as banking information, personal or business identification, credit card data and transportation passes. These cell phone devices can function as both a digital wallet and a communication device. The first unit is called the P506iC and it was released in July 2004. Soon after the introduction of SH506iC, more sophisticated units are expected to follow.

Inside the DoCoMo phone sets, there are microchips developed by Sony, known as FeliCa or iMode FeliCa. The chip is capable of storing large amount of data and can perform necessary processing and communications functions. It allows users to perform several transactions on the fly – for example, users can upload digital cash from a credit card, or pass a phone set near a scanning device at a department store checkout station. What is more, users can also use their phone set as a virtual train ticket. In addition to these fancy functions, the cell phone units can also be used for routine calling and they also have E-Mail functions, and can be used for sending and receiving images. All this is in addition to performing the smart-card-equivalent functions. And there is more than that! 3G DoCoMo phone sets, operating with 3G, are expected to provide remote or automatic locking. With this feature, if a phone unit is lost or stolen, unauthorized persons cannot use it. Currently, this standard is found only in Japan. NTT DoCoMo phones are considered to be very advanced in terms of technology. They, of course, support text and picture messaging.

Other Standards

Besides the major mobile phone standards mentioned above, there are other standards as well used far less frequently including NAMPS, iDEN/Nextel, NMT, TETRA/Dolphin, Iridium and Globalstar. IMU has no direct support for these standards, but may still be able to receive messages sent by one of these, provided that the carriers have interoperability agreements with GSM or CDMA operators, or provided that IMU can be directly connected to a message server on one of these networks.

Following are the links provided for GSM tutorials to aid those who are not familiar with it:

<http://www.palowireless.com/gsm/tutorials.asp> (26 April 2010).

<http://www.tutorialspoint.com/gsm/index.htm> (26 April 2010).

[\(26 April 2010\).](http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm_introduction.php)

8.2.2 NTT DoCoMo

Digital Advanced Mobile Phone Service (D-AMPS) is the digital version of the original analog standard for cellular telephone phone service. Now “Do Communication over the Mobile Network” (DoCoMo) is also available. NTT DoCoMo is Japan’s largest wireless network carrier. They offer a service known as 2G Personal Digital Cellular (PDC – it is TDMA-based; see Box 8.1). NTT DoCoMo was the first in the world to offer 3G service^[2] with their WCDMA-based Freedom of Mobile Multimedia Access (FOMA) network. Wideband Code Division Multiple Access (WCDMA) is used across the world in various countries. It is most prominently used in Asia and Europe. WCDMA implementation is different although it is based on CDMA: CDMA uses one or more 1.25 MHz channels whereas WCDMA uses two 5 MHz channels. NTT DoCoMo is the developer and licensor of the iMode Internet browsing system for mobile phones. The discussion about cellular network organization is beyond the scope of this chapter. Readers can refer to any standard text devoted to this topic.

Mobile phones are highly powerful communications devices. They can perform a number of functions. The capabilities of modern mobile phones range from those of a simple digital organizer to those of a low-end PC. Designed for mobility (to promote remote working), they are compact in size, battery powered and lightweight.

Most cell phones are featured with a basic set of comparable functionalities and capabilities. They house a microprocessor, read-only memory (ROM), RAM, a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD). The device has its operating system (OS) resided in ROM, which can be typically erased and reprogrammed electronically with proper tools. RAM, which for certain models may be used to store user data, is kept active by batteries, whose failure or exhaustion causes that information to be lost. Modern cell phones are equipped with system-level microprocessors – with this the number of supporting chips required gets reduced and a considerable memory capacity gets added. There are built-in mini secure digital (MiniSD), multimedia card mobile (MMCmobile) or other types of card slots to support removable memory cards. There are also specialized peripherals, such as an SDIO Wi-Fi card. Wireless communications such as infrared (i.e., IrDA) or Bluetooth may also be built into the device.

Box 8.2

Mobile Handsets Challenges – Tracing Call Logs and Retrieving Information

As one can imagine, a huge variety of data can be extracted from mobile handsets. Mobile phones can contain a large amount of information covering a vast array of technologies. There are two main areas that can be analyzed: phone data and data found on the Subscriber Identification Module (SIM). Inside the internal memory of a mobile phone many different types of information can be stored; for example, short dial numbers, text messages, settings (language, date/time, tone/volume, etc.), stored audio recordings, stored computer files(i.e., pictures and graphics), logged incoming calls and dialled numbers, calendar entries and possible events, bookmarks, GPRS, WAP and Internet settings, etc.

However, mobile phones do pose multiple issues that need to be addressed to ensure the integrity and reliability of forensics testing. For example, there can be issues involving data security, the need to ensure data recovery and other variables that could potentially compromise evidence. Initially, all phones used to have a unique identifier number. This number started at 001 and increased in increments of one for each new handset, that is, 001, 002, 003, etc. This ensured that each handset could be located quickly and easily and ensured that it would not get contaminated.

Box 8.2 Mobile Handsets . . . (Continued)

When a new SIM card is put inside a GSM handset, the call logs on most GSM phones cannot be recovered. The call logs are supposed to store information about calls received and calls missed as well as information about calls made by the user. These logs get reset when a new SIM card is inserted into a handset. Let us consider a scenario – suppose, a particular SIM card is removed from the handset and then later it is put back into the handset. Furthermore, no other SIM card is inserted into the handset in between. Under such a scenario, memory will not be erased. However, upon inserting a different card, the call logs will get erased. To the best of our knowledge, currently there are no known forensics software tools available to deal either with “undeleting” or for recovering deleted data from mobile handsets. One widely known method of extracting this data from handsets is to first image the memory from the handset to a computer and then carry out forensics analysis of the image using tools such as Encase to extract the data. As mentioned in Chapter 7, “imaging” means converting the entire memory into a single searchable file.

Another challenge is presented by the network connectivity aspect. Owing to the nature of mobile phones they are almost always on and connected to a network. This means that messages and calls can be sent and received. The first step to be performed on a “seized” mobile handset is to protect that handset from the network to ensure that new data cannot be sent to, or from, the device which could change the memory from the time of seizure and potentially delete other data that could be used as evidence. To secure devices this way they should be immediately switched OFF to prevent access to the mobile network. When turning the device back ON, a Faraday bag (see Fig. 8.2) or other similar apparatus should be used to prevent the device from connecting to the outside mobile network.



Figure 8.2 | Faraday bags.

Sources: <http://www.faradaybag.com> (20 April 2010); <http://www.textually.org> (20 April 2010); <http://www.innotechprod.com> (20 April 2010); <http://www.libertypkg.com> (20 April 2010).

8.2.3 Cell Phones: Hardware and Software Features

Different devices have different technical and physical features/characteristics (e.g., size, weight, processor speed and memory capacity). Devices may also use different types of expansion capabilities to provide additional functionality.



Cell phone capabilities sometimes include those of other devices such as personal digital assistants (PDAs), global positioning systems (GPS) and cameras.

Overall, they can be classified as basic phones, that is, used primarily as simple voice and messaging communication devices; advanced phones that offer additional capabilities and services for multimedia; and Smartphones or high-end phones that merge the capabilities of an advanced phone with those of a personal digital assistant (PDA). Table 8.1 highlights the general hardware characteristics of basic, advanced and Smartphone models, which underscore this diversity. The characteristics used in this classification scheme are only illustrative – the features of actual devices may vary and may possess more than one category identified. With passage of time, advanced features also tend to appear in more basic phones as new ones are added to the high end. Although the lines among this classification scheme are somewhat fuzzy and dynamic, it, nevertheless, serves as a general guide.



Irrespective of a cell phone type, all devices support voice and text messaging, a set of basic personal information management (PIM) applications including phonebook and date book facilities, and a means to synchronize PIM data with a desktop computer. More advanced devices also provide the ability to perform multimedia messaging, connect to the Internet and surf the Web, exchange E-Mail or chat using instant messaging. They may also provide enhanced PIM applications that work with specialized built-in hardware, such as a camera.

Table 8.1 | Hardware characteristics: Hand-held devices

	<i>Basic</i>	<i>Advanced</i>	<i>Smart</i>
Processor	Limited speed	Improved speed	Superior speed
Memory	Limited capacity	Improved capacity	Superior capacity, built-in hard drive option
Display	Gray scale	Color	Large size, 16-bit color (65536 colors) or higher
Card slots	None	MiniSD or MMCmobile	MiniSDIO or MMCmobile
Camera	None	Still	Still, Video
Text input	Numeric keypad	Numeric keypad, soft keyboard	Touchscreen, handwriting recognition, built-in QWERTY-style keyboard
Cell interface	Voice and limited data	Voice and high-speed data	Voice and very high-speed data
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, Wi-Fi
Battery	Fixed, rechargeable lithium ion polymer	Removable, rechargeable lithium ion polymer	Removable, rechargeable lithium ion polymer

Table 8.2 | Software characteristics: Hand-held devices

	<i>Basic</i>	<i>Advanced</i>	<i>Smart</i>
OS	Proprietary	Proprietary	Linux, Windows Mobile, RIM OS, Palm OS, Symbian
PIM	Simple phonebook	Phonebook and Calendar	Reminder list, enhanced phonebook and calendar
Applications	None	MP3 player	MP3 player, Office Document Viewing
Messaging	Text messaging	Text with simple embedded images and sounds (enhanced text)	Text, enhanced text, full multimedia messaging
Chat	None	SMS chat	Instant messaging
E-Mail	None	Via network operator's service gateway	Via POP or IMAP server
Web	None	Via WAP gateway	Direct HTTP
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, Wi-Fi

“Smartphones” are very high-end devices – they possess PDA-like capability for reviewing electronic documents (e.g., reports, briefing slides and spreadsheets). Smartphones are capable of running a wide variety of general and special purpose applications. Smartphones are typically larger than other phones and they support a bigger form factor, that is, size display, etc. Smartphones may also have an integrated QWERTY keyboard or touch-sensitive screen. They also offer more extended expansion capabilities through peripheral card slots, other built-in wireless communications such as Bluetooth and Wi-Fi and synchronization protocols to exchange other kinds of data beyond basic PIM data (e.g., graphics, audio and archive file formats). Table 8.2 lists the differences in software capabilities found on these hand-held device classes.

8.3 Hand-Held Devices and Digital Forensics

There is no dearth of hand-held devices in the modern world of today. The use of these devices is rampant given the modern lifestyles in our digital economy. Figure 8.1 in the introduction section shows some hand-held devices. Device forensics is a branch of computer forensics; it deals with gathering digital evidence available in different types of devices such as mobile phones, PDA, iPod, printers, scanners, camera, fax machines, etc. The normal computer forensics procedure is inadequate to identify and collect the evidence from these devices. Sound forensics techniques along with systematic approach are essential for collecting evidence in such devices and to ensure its admissibility in a court of law.



“Device forensics” has many aspects such as *mobile phone forensics*, *PDA forensics*, *digital music forensics*, *iPod forensics* and *printer and scanner forensics*.

Let us take a brief look at each of these. Considering that iPods are relatively new devices joining the market, forensic aspects of iPod are addressed in Section 8.5.

Box 8.3 Hand-Held Devices and Digital Forensics

Recall the discussion in Chapter 3 about use of hand-held devices in committing cybercrimes. There is a proliferation of hand-held devices in today's world. Mobile workforce is on the rise and information coming in from mobile devices is of great value nowadays. Cell phones, Smartphones and other mobile devices play significant role in our life. People tend to store a lot of important information there: telephone numbers, addresses, photos, E-Mails, notes, messages, calls history, voice records, videos, etc. The growth, in the size and type of data stored in mobile devices, means that fast, convenient and thorough data analysis is now crucial like never before. It is amazing to know the varied products in the market place; more than 1,350 mobile device models are supported. And the list is rapidly growing!

"Device seizure" comes as the first line of defense in hand-held forensics. The amount and quality of data that one can obtain from a full physical acquisition far exceeds the information one can obtain from a simple logical acquisition. Accessing phones via IrDA and Bluetooth is recommended for use only when other data connections are not available – possibly due to the lack of security in these communication methods. Unlike in the past, now there is technical support available for more devices. Symbian 6.0 support is also now available. In this paradigm, a forensics investigator would like to have the toolbox with sevice seizure added to the repertoire. By their very design, "device seizure" toolboxes come as a collection of the forensics features needed in different scenarios of investigation. Those features in such toolboxes, combined with the appropriate software, allow for acquisitions of hundreds of mobile phones and PDAs.

By seizing the hand-held device used for crime, one can acquire the following data:

1. SMS history (text messages)
2. Deleted SMS (text messages)
3. Phonebook (both stored in the memory of the phone and on the SIM card)
4. Call history
 - Received calls;
 - dialled numbers;
 - missed calls;
 - call dates and durations.
5. Datebook
6. Scheduler
7. Calendar
8. To-do list
9. File system (physical memory dumps)
 - System files
 - Multimedia files (images, videos, etc.)
 - Java files
 - Deleted data
 - Quicknotes, etc.
 - GPS waypoints, tracks, routes, etc.
 - RAM/ROM
10. PDA Databases
11. E-Mail
12. Registry (Windows Mobile devices)

The following links are useful for some additional and related information:

You can see some video clips by visiting the URL at www.paraben-forensics.com

You can contact at the following site to obtain a registered product:

<http://www.paraben.com/programs/demo.php> (5 September 2009).

You can also visit the link for Device Seizure Toolbox at:

<http://www.dataduplication.co.uk/pdfs/Device%20Seizure%20Toolbox%20Feb09.pdf>

8.3.1 Mobile Phone Forensics



Mobile phone or cell phone is the most familiar hand-held device because it is the most ubiquitous one. Nathan B. Stubblefield invented and patented the first mobile telephone 100 years ago.

As mentioned before, modern cell phones are highly mobile communications devices designed to perform a range of functions – from that of a simple digital organizer to that of a low-end PC. Designed for mobility, they are compact in size, battery powered and lightweight, often use proprietary interfaces or OS and may have unique hardware characteristics for product differentiation.



“Mobile phone forensics” is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

Mobile telephone forensics and evidence has not developed overnight; it has been developing from the earliest building blocks of scientific discovery back in the 19th century. Mobile phones, in particular, those with advanced capabilities, are a relatively recent phenomenon. They usually are not covered in classical computer forensics. Cell phones vary in design and are continually evolving in terms of functionality and features as current technologies continue to become obsolete and new technologies are introduced. We need to develop an understanding of the components and organization of cell phones in order to understand the criticalities involved when dealing with them forensically. Similarly, features of cellular networks constitute a crucial aspect of cell phone forensics, since logs of usage and other data are maintained there.

Cell phone forensics includes the analysis of both SIM and phone memory; each requires separate procedure to deal with.



The “IMEI number” (International Mobile Equipment Identity) of a cell phone is a very important starting point for the First Information Report (FIR) procedure as the FIR would most probably require the IMEI number as the basis when a compliant about a lost/stolen mobile phone is to be registered with the police. This is because a cell phone can be traced with its IMEI number.

Every time a cell phone is switched ON or a call is made, the IMEI number is transmitted out to the network provider where it gets tallied against an information directory called Equipment Identity Register (EIR). Using the EIR information, a telecom company can locate a particular cell phone by pinpointing its proximity to the nearest tower. In special cases like theft, the telecom company can also block the particular cell phone reducing it to a piece of plastic junk. Box 8.4 provides some smart tips.

Box 8.4 Cell Phone – Smart Tips

Many of you must be aware of the following:

1. You will find the International Mobile Equipment Identify (IMEI) number of your cell phone when you open the back battery cover and remove the battery. In some mobiles, the IMEI number is printed just below the battery slot. The IMEI number is a 15-digit number without dots or dashes. If it is not there do not panic, just follow step 2 to know your IMEI number.
2. Switch on your mobile after replacing the battery. Enter the following numbers in sequence “*#06#” (or any other applicable digit/symbol sequence depending on the type of handset you are using) with or without the quotes and you will see the 15-digit IMEI number on the screen. Similarly, when you enter “*#0000#” (without the quotes of course), the information about the type of your cell phone is displayed.
3. Note down this number for reference. Although this method is common for most, some brands could have a different method to access this number. Consult the cell phone guide or call your customer care to find out the way.

There are a few tips to enhance the safety of your cell phone :

1. Note down your IMEI number and record it in a safe place.
2. Report any theft of a stolen phone immediately and file an FIR at the nearest police station.
3. Get the IMEI number verified from your operator whenever you buy a used phone.
4. Phones without IMEI number should not be used, as they are not safe from security perspective

Refer to article in Ref #19, Articles and Research Papers, Further Reading.

A point to note is that not all activities with a mobile phone lead to impact on the radio and fixed mobile network. Recall discussion in Section 7.5 Cyberforensics and Digital Evidence – network records are not limited to billing records; therefore cell site analysis should not be excluded when you are considering this model. There may not be parity between data obtained from the mobile telephone and the network records and vice versa. Cell phone tools and SIM tools are summarized in Table 8.3. While going through this table, recall Section 7.7.2 of Chapter 7 to refresh your memory about the phases in computer forensics/digital forensics.

It helps to clarify some terms in relation to mobile devices. In the context of the discussion here, the use of “mobile devices” does not refer to thumb drives, universal serial bus (USB) drives, memory sticks, portable flash drives or portable externally enclosed hard drives. Mobile devices specifically refer to cellular (or mobile) phones, PDAs and Smartphones. Bear in mind that some of the older model PDAs, such as the initial Palm and BlackBerry series devices, do not have radio (cellular) capability and are simply used to store personal information (contacts, calendars, memos, to-do lists, etc.)

Mobile device representation comes in various forms:

1. Cellular phones
 - CDMA: typically handset only;
 - GSM: handset and SIM;
 - iDEN: handset and SIM.
2. PDAs
 - Palm Pilots (Palm OS);
 - Pocket PC's (Windows CE, Windows Mobile);
 - BlackBerry's (RIM OS) that contain no radio (cellular) capability;
 - others (Linux, Newton).
3. Smartphones: They are the hybrid between 1 and 2 have radio capability (see Section 8.3.5).

Table 8.3 | Cell phone tools and SIM tools

Name of the Tool	Forensics Phases Supported	Features
<i>Cell Phone Tools</i>		
PDA seizure	Acquisition, examination, reporting	<ul style="list-style-type: none"> Targets Palm OS, Pocket PC and RIM OS phones No support for recovering SIM information Supports only cable interface.
Pilot link	Acquisition	<ul style="list-style-type: none"> Targets Palm OS phones Open-source non-forensics software No support for recovering SIM information
Cell seizure	Acquisition, examination, reporting	<ul style="list-style-type: none"> Supports only cable interface. Targets certain models of GSM, TDMA and CDMA phones Supports recovery of internal and external SIM Supports only cable interface
GSM.XRY	Acquisition, examination, reporting	<ul style="list-style-type: none"> Targets certain models of GSM phones Supports recovery of internal and external SIM Supports cable, Bluetooth and IR interfaces
Oxygen Phone Manager (OPM – forensics version)	Acquisition, examination, reporting	<ul style="list-style-type: none"> Targets certain models of GSM phones Supports only internal SIM acquisition
<i>Note:</i> OPM was initially designed as an agent for users to edit the information stored on their handsets through their computers. However, OPM has been expanded and now individually caters for Nokia- and Symbian-based handsets in separate versions, as well as having forensics editions designed to investigate handsets without corrupting any data on the device. Owing to monetary constraints access to OPM 2, Forensic Edition for Nokia Devices could not be obtained; however, a trial version of the phone manager was used for a basic idea of how OPM works. The major problem with this was that any testing carried out on handsets could not be verified, nor used in any investigation because this version was designed to allow data to be manipulated that goes against the methodology of forensics investigations.		

(Continued)

Table 8.3 | (Continued)

Name of the Tool	Forensics Phases Supported	Features
MOBILedit! Forensic	Acquisition, examination, reporting	<ul style="list-style-type: none"> Targets certain models of GSM phones Provides internal and external SIM support Supports cable and IR interfaces
Cell seizure	Acquisition, analysis/examination	<ul style="list-style-type: none"> Designed by Paraben forensics Specifically designed for forensics use and acquisition on the more popular brands of older Nokia, Siemens, Motorola and SonyEricson phones Simple to use
BitPIM	Acquisition, examination	<ul style="list-style-type: none"> Targets certain models of CDMA phones Open-source software with write-blocking capabilities No support for recovering SIM information
TULP 2G	Acquisition, reporting	<ul style="list-style-type: none"> Targets GSM and CDMA phones that use the supported protocols to establish connectivity Provides internal and external SIM support Requires PC/SC-compatible smart card reader for external SIM cards Supports cable, Bluetooth and IR interfaces

(Continued)

Table 8.3 | (Continued)

<i>Name of the Tool</i>	<i>Forensics Phases Supported</i>	<i>Features</i>
<i>SIM Tools</i>		
Cell seizure	Acquisition, examination, reporting	Also recovers information from SIM card when inserted in handset
TULP 2G	Acquisition, reporting	Also recovers information from SIM card when inserted in handset
GSM .XRY	Acquisition, examination, reporting	Also recovers information from SIM card when inserted in handset
MOBILedit! Forensic	Acquisition, examination, reporting	Also recovers information from SIM card when inserted in handset
SIMIS	Acquisition, examination, reporting	External SIM cards only
ForensicSIM	Acquisition, examination, reporting	External SIM cards only Produces physical facsimiles of SIM for prosecutor and defense, and as a storage record
Forensic Card Reader	Acquisition, reporting	• External SIM cards only
SIMCon	Acquisition, examination, reporting	• External SIM cards only

With the emergence of Smartphone devices the cell phone and data storage organizer distinctions are now becoming blurred (refer to Fig. 8.1). These devices encompass the features of cell phones (radio capability) and the ability to store personal data, surf the Web, send text messages (short message service, SMS) and/or multimedia messages (MMS), check E-Mail, instant message (IM), make audio or video calls, download/upload content to and from the Internet, take pictures as well as video. Essentially, a mobile device can do much of what a computer or laptop can do, just on a smaller scale. Those with a computer forensics background, perhaps already realize the breadth of information that can be locally stored on these small-scale digital devices.

8.3.2 PDA Forensics



Personal digital assistant (PDA) is also referred to as “palm device” or “hand-held.” The most common operating system (OS) used are the Palm OS (Palm, Sony, Handspring), Windows for Palm (HP), MS Pocket PC (Compaq), Embedix (Sharp).

PDAs are getting immensely popular. PDAs are no longer just electronic devices holding personal information, appointments and address book. Modern PDAs are hybrid devices integrating wireless, Bluetooth, infrared, Wi-Fi, mobile phone, camera, GPS, basic computing capabilities, Internet, etc., in addition to the standard PIM features. Technology is often a “double-edged sword” and it breeds crime. PDAs are also no exception; criminals are increasingly using them in committing electronic crimes; given the compact size and integrated features of PDAs, it becomes convenient for criminals to use them. There is indeed an issue of growing crimes involving portable devices (see Chapter 3).

A PDA has many components. A major component of PDA is the microprocessor; all PDA devices have to have some form of a microprocessor. The microprocessor, inside a PDA, is similar to any microprocessor; the only difference is that it has a restriction on the size as it has to reside in the pocket-sized PDA. Another important component of the PDA is its input device and it can vary in its form. One of the most common method of input, these days, is the touchscreen. In addition to these components, an essential component is the OS that is running the software for the PDA device.



PDAs differ in several important ways compared with PCs. PDAs vary in areas of OS, interface style and hardware components, and they work with different OS such as Linux, Palm OS and Microsoft Pocket PC.

Basically, a PDA contains a processor, RAM, ROM and other ports for connecting the PDA to a computer system. The ROM stores the OS of the PDA and other information that should not be altered, whereas the RAM stores the handler's data and works with battery power whose failure causes the information to be lost. Compact flash and secure digital slots assist cards of memory and wireless communication. Users mainly use PDAs for storing data in various file formats, access the Internet, send and receive E-Mails. PDAs have PIM applications that consist of calendar, task management, contacts and E-Mail software. PDAs can be synchronized with a PC by using software such as Microsoft Pocket PC ActiveSync, HotSync from Palm, etc. Owing to the design and architecture, PDAs require specialized forensics tools and procedures that are distinct from tools used for single PC systems and network servers. Hackers used to attack PCs and servers of organizations to destroy the data. With users using more and more hand-held devices, now the

Table 8.4 | PDA forensics tools

<i>OS on Which it Works → Tool Name (See Below)</i>	<i>Palm OS</i>	<i>Pocket PC</i>	<i>Linux</i>
PDA seizure	Acquisition, examination, reporting	Acquisition, examination, reporting	NA
EnCase	Acquisition, examination, reporting	NA	Examination, reporting
Palm DD (PDD)	Acquisition	NA	NA
Pilot link	Acquisition	NA	NA
POSE	Examination, reporting	NA	NA
dd	NA	NA	Acquisition

Note: The command “dd” is an extremely powerful copy program found on most versions of Unix or Linux. The command dd can copy a file or device to another file or device. The output generated by dd is extremely versatile as it is understood by most, if not all, forensics examining tools, commercial or open source.

Note: The abbreviation NA means that the tool at the left of the row is not applicable to the device at top of the column.

problems of hacking, viruses, Trojans and worms have spread to these devices. Hackers can hack these devices or use these devices, instead of using a computer, to hack users' devices or other computers. Therefore, there exists a need for having forensics tools not only for computers but also for these devices. PDA forensics tools are listed in Table 8.4. The forensics phase supported by each of those tools is mentioned in the last three columns.

When it comes to forensics tools for PDAs, the situation is different in the case of PCs; there is a limited number and variety of toolkits for PDAs. Not only are there fewer specialized tools and toolkits, but also a range of devices over which they operate is typically narrowed to only the most popular families of PDA devices – those based on the Pocket PC and Palm OS. Moreover, the tools require that the examiner has full access to the device (i.e., the device is not protected by some authentication mechanism or the examiner can satisfy any authentication mechanism encountered). Although a couple of toolkits support a full range of acquisition, examination and reporting functions, the remaining tools focus mainly on a single function.



Investigating crimes involving PDAs are more challenging than those involving normal computers. This is mainly because these devices are more compact, battery operated and store data in volatile memory.

As long as the PDA has sufficient battery power, it is can be turned ON. Evidence residing in PDA is of highly volatile in nature – so volatile that one can easily alter the evidence or damage it without that getting noticed. Sound forensics techniques combined with a systematic approach are required for collecting the

evidence residing on a PDA and also for ensuring the admissibility of that evidence in a court of law. For investigation of digital crimes through use of PDAs, a standard forensics model is needed as an abstract reference framework. Not only the law enforcement officials but also IT auditors, information security experts, IT managers and system administrators can benefit from such a model – they often are one of the first responders related to any sort of computer crime in an organization.

Relevant software in this segment is listed below:

1. **PDD:** It is based on the Unix dd. This is the most popular Palm forensics software. To know more on this, visit: <http://www.forensicswiki.org/wiki/PDAs>
2. **CodeWarrior for Palm OS:** It is used to put palm devices into “Debug Mode.” This allows communication via serial port, imaging and can be used to overcome lockout protection. To know more on this, visit the link: <http://www.codewarrior.com/products/palm>
3. **PDA defense:** It is a third-party lockout software. It is difficult to bypass. To know more on this, visit: <http://www.pdadefense.com/palm.asp>



Forensics tools acquire data from a device in one of the following two ways: “physical acquisition” and “logical acquisition.”

Physical acquisition works as a bit-by-bit copy of an entire physical store (e.g., a disk drive or RAM chip), while logical acquisition involves a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., involving several disk drives). The difference lies in the way of seeing the memory, that is, the difference in how the OS sees the memory (i.e., a logical view) as compared to how the processor or other related hardware components see the memory (i.e., a physical view). In general, physical acquisition is preferable. This is because during the forensics examination process, it does not get impacted by the presence of any leftover data bits and bytes (e.g., unallocated RAM, unused file system space, etc.) in a logical acquisition, such leftover data pieces would otherwise go unaccounted for. In general, it is easier to import physical device images into another tool for examination and reporting. On the other hand, with logical acquisition it becomes easier and more natural to understand the organization of the information acquired. Both methods of acquisition are therefore preferable, if the situation permits it.

8.3.3 Printer Forensics

One may wonder how printers can pose security risks. Printers are not generally considered to be “hand-held” devices although “portable printers” are now available in the market. We discuss printer forensics here because this chapter is about “device forensics” and other devices addressed for discussion are “hand-held” devices. Printers too present security challenges; printers are no more than just dump devices especially in the network printer era. Many organizations, which otherwise have reasonably good security practices, tend to completely neglect their network printers. As per usual working practice, printers are simply installed and, as long as they work, nobody pays any attention to them until it is time to reload the paper or replace the toner cartridge. It should be noted that most of these printers are “dormant bombs,” ripe for any simple attack by even the most novice hacker.



Modern day printers have computer-like characteristics with internal storage, FTP uploading, Simple Network Management Protocol (SNMP), etc. Some printers are loaded with vulnerable applications.

Some printers even have embedded Windows systems that are interfacing with the network. Yet, as author's audit experience in the IT industry shows, almost no risk management or oversight is used to protect the printers from attacks. Most of the multifunction printers can perform one or more of the these tasks – sending E-Mail, sending fax, printing, photocopying, stapling/collating/stacking, etc. Printers are in the same vulnerable position as most of the network devices. Confidential/sensitive data can flow to printers which often escape security attention. At a minimum, hackers can access classified information sent to the printer. At worst, they can be turned into remote-controlled Bots and be used as a launching pad for further attacks. Possible attacks through printer exploits are as follows:

1. Modifying IP address of the printer to an unused address on the same subnet.
2. Changing IP address of the target machine to the previous IP address of the printer.
3. Capturing all traffic sent over Port 9100^[3] to the IP address to which end-users are configured to print. The attacker can keep collecting print jobs until it is found out.
4. Forwarding all print jobs onto the “new” IP address of the printer; when the end-user who submitted the job goes to the printer in question to collect the print job, he/she finds that it has been processed as normal.

All this happens so fast that the end-user would hardly suspect anything.

Visions of “paperless” office were projected many years back and yet offices continue to be loaded with papers! Despite the increase in E-Mail and other forms of digital communication, the use of printed documents continues to increase every year. Printed material often comes handy as a useful accessory to many criminals and terrorist acts; for example, document forgery or document alteration used for purposes of identity theft, security or recording transactions. In addition, printed material may be used in the course of conducting illicit or terrorist activities. Also, common users need to be able to print secure documents, for example, boarding passes and bank transactions. In both cases, the ability to identify the device or type of device that used to print the material in question would provide a valuable aid for law enforcement and intelligence agencies. For example, counterfeiters often digitally scan currency and then use color laser and inkjet printers to produce bogus bills. Forgers use the same methods to prepare fake passports and other documents. Investigators would like to determine that a fake invoice or any other business document is created on a certain brand and model of printer. They would also be interested in identifying not only the model of the printer used for the crime but also which particular printer was used in the criminal act. Thus, it should be possible to know the difference between counterfeit invoices created on specific printers even if they are of the same model. There are two possible approaches. In the first approach one analyzes a document for identifying the characteristics that are unique to each printer. The second approach is designing printers to purposely embed individualized characteristics in documents. The second method is followed by most of the latest printer manufacturing companies.



No two printers of the same model will behave in the exact same pattern. This is because the mechanical parts that make the printer will not be 100% equivalent.

Manufacturing such printers that have 100% equivalent mechanical parts would be too expensive for consumers. If, however, the printer cartridge is changed after a document is printed, the document no longer can be traced to that printer.

8.3.4 Scanner Forensics

Today, a large portion of digital image data is available. Acquisition devices such as digital cameras and scanners are used to create that data. With cameras, it is possible to digitally reproduce scenes that may look almost as real as natural scenes. Even while cameras are useful reproduction devices, scanners are used for capturing hardcopy art in more controlled scenarios. For a sound forensics approach, one needs a non-intrusive method for scanner model identification. Moreover, authentication of scanned images is a necessity in most forensics scenarios. Even if only scanned image samples are used, with a robust scanner identifier it should be possible to determine the brand/model of the scanner used to capture individual scanned images. An approach for such scanner identification is based on statistical features of scanning noise. Scanning noise of the images can be done from multiple perspectives, including image de-noising, wavelet analysis, and neighborhood prediction, and one can obtain statistical features from each characterization.

One can apply the same approach to digital cameras and other imaging devices. The most significant challenge is that analytical procedures and protocols are not standardized nor do practitioners and researchers use standard terminology. As a result of continuously changing technology, there will always be new devices in the digital world. Whenever a new digital device enters the market, a forensics methodology has to evolve to deal with it. This phenomenon will expand the field of device forensics.

8.3.5 Smartphone Forensics

Workforce mobility is on the rise and Smartphones are gaining momentum as a device option for people working at the field (field workers include, e.g., sales personnel, technicians, insurance agents, medical officers, pathological laboratory technicians who offer door-to-door medical service, etc.). The main reason for rising popularity of Smartphones is their high functionality that comes in a relatively low-cost device.



Smartphones are mobile phones based on high-level OS that are open to third-party application development.

Mass market availability of Smartphones has created a wide variety of affordable form factors that span the continuum of voice vs. data-centric designs. The market for Smartphones is growing rapidly, better than that for mobile phone market (see Fig. 8.3).

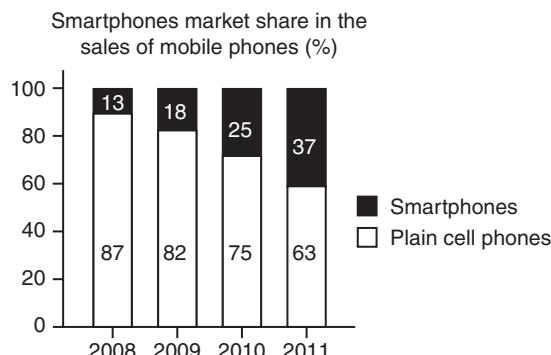


Figure 8.3 | Smartphones market is growing even when general mobile phones market is falling.
Source: <http://www.oxygen-forensic.com>

Feature-wise, a “Smartphone” is a hand-held PC. It has various facilities:

1. It works as a cell phone.
2. It has got a full-fledged address book, a planner, an organizer, messenger, photo and video camera.
3. It has GPS navigation facility.
4. It works as a Web Client to access Web-based applications.
5. It is a platform for third-party applications.

Enterprises evaluate Smartphones as the main device for certain types of field workers for the following three reasons:

1. They have an always-connected status.
2. They have the ability to act as a user’s primary communication terminal.
3. They can be the platform for mobilizing enterprise applications.

Therefore, let us understand these aspects of Smartphone in terms of what kind of information they can contain from forensics angle.

As a “cell phone,” a Smartphone has the basic information such as IMEI number (see Box 8.4 and Section 8.3.1), hardware and software version numbers with which the phone operates, and network information. The event log of Smartphone includes records of events such as incoming and outgoing calls, missed calls history, sent and received messages history, GPRS and Wi-Fi sessions, etc. The SIM card of a Smartphone contains the International Mobile Subscriber Identity (IMSI), phone numbers and SMS messages, although usually these features are not utilized by Smartphones. The address book in the Smartphone can hold this information as part of contacts information – name fields (first, middle, last), nickname, prefix, suffix, joint name, photo and personal ringing tone, phone numbers (general, mobile, fax, video, pager, VoIP, push-to-talk), postal addresses, webpages and E-Mail addresses, company, department, job title, text notes, private information (birthday, spouse, children), custom field labels, multiple fields of the same type, last modification date and time. Caller group information and assigned speed dial information is also there in the Smartphone.



There is much more inside the Smartphone than that mentioned above. People tend to use the “planner” feature of Smartphone to store their meeting details, reminders and anniversaries and in the process a lot of “Metadata” (data about this data) gets stored too.

The planner in the Smartphone also has people’s task-related information (task description, deadlines, priority, completion time and date, etc.). Besides lost personal and sensitive information in the event of the Smartphone being stolen, it also gives avenues to investigator for forensics analysis in the case of crimes. The messenger feature of the Smartphone also brings a wealth of information to forensics analysts/investigators – for example, information such as text messages (SMS), multimedia messages (MMS), E-Mail messages with attached files, beamed messages: files sent via Bluetooth, IR or USB, standard message folders, custom message folders, date and time, service center timestamp information about deleted SMS messages, etc. As some of the Smartphone models contain the GPS navigation feature too, forensics examiners can use that feature to learn about the movement of the criminal in cases where it is believed or known that the criminal used his/her Smartphone.

We can understand how cookies can give a lot of clues to forensics investigators and it is when computer is used for crimes. Now that computer features get extended to hand-held devices, Smartphones are almost the hand-held computers! The Web Client of the Smartphone holds forensically useful information such as web cache files, bookmarks, pages view history, last opened URLs, search history and cookies (more about

cookies in Chapter 9). The IM client on the Smartphone holds information such as IP, Login (UID, E-Mail) and password, contacts list, chat history and calls history. We have mentioned that Smartphones are hand-held PCs – as such, they also contain camera snapshots, video clips, voice records, sounds and Podcasts, Wi-Fi networks list, paired Bluetooth devices list, activated SIM cards list and VPN profiles. As part of third-party applications installed on the Smartphone, forensics can find the list of installed applications, office documents, application logs and data files.

Logical analysis of data extracted from Smartphones, involves data extracted using common PC-to-mobile communication protocols: AT, OBEX, SyncML and Smartphone connected to PC with a standard cable (or Bluetooth/IR adapter). Physical analysis involves data extracted using direct memory reading (hex dump) and Smartphone (or its memory chip only) connected to special hardware (see Fig. 8.4).

In Fig. 8.4, it is to be noted that OBEX, SyncML, AT-commands, etc. are modern protocols originally developed for data synchronization. When it comes to Smartphones, standard protocols can extract only a little bit of digital evidence, the tip of the iceberg, so to speak. However, now, Oxygen Forensic software tools offer affordable, easy, yet technically sophisticated tool to get the maximum of evidential content from handsets, especially Smartphones. Also refer to Table 8.3; the new Oxygen Forensic Suite incorporates Oxygen's breakthrough technology for the total extraction of critical data from the most popular cell phones, including Nokia, Sony Ericsson, Samsung, Motorola, Vertu and Smartphones powered by Symbian OS, Windows Mobile and BlackBerry. The program automatically performs forensics extraction of data such as

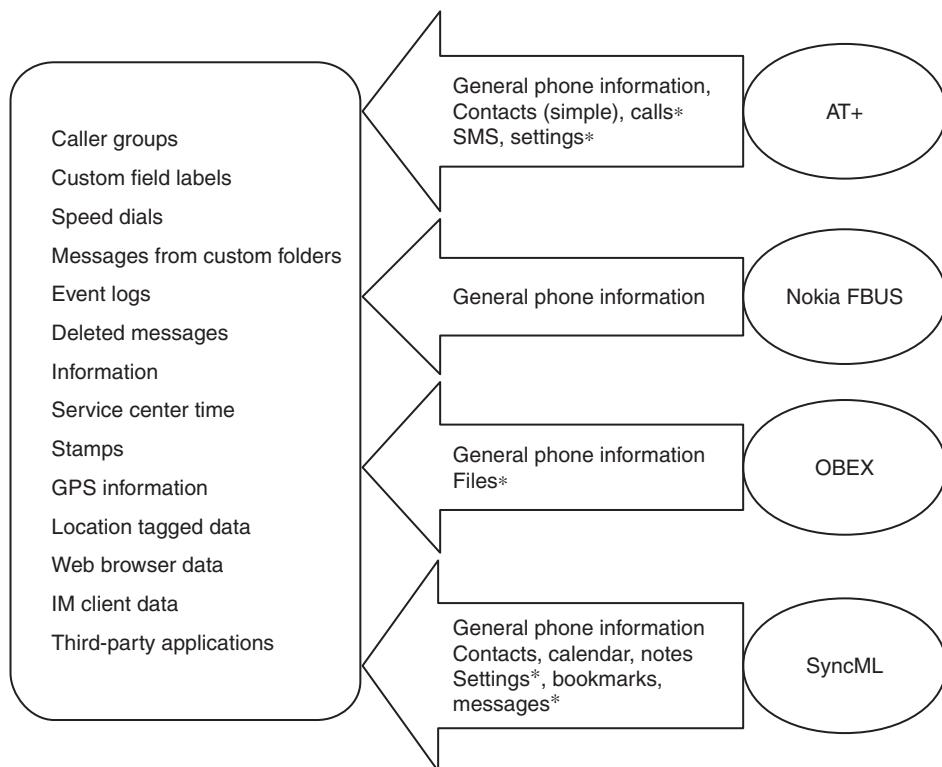


Figure 8.4 | Logical analysis of Smartphones.

Note: “*” indicates that the available data set is highly dependent on manufacturer’s implementation.

general phone information and SIM card data; address book; caller groups data; calendar events; text notes; incoming, outgoing and missed calls history, including time and duration; GPRS, EDGE, CSD, HSCSD and Wi-Fi traffic and sessions log; SMS, MMS and E-Mail messages, including the messages from custom folders; deleted SMS information (with some restrictions); camera snapshots, video clips and voice records; files and directories from the phone memory as well as from flash card; list of installed applications such as Java as well as native Smartphone applications; and list of tuned FM radio stations.

8.3.6 iPhone Forensics



The iPhone was introduced by Apple Inc. in January 2007. Since then, Apple has sold more than 33 million iPhones and has now surpassed RIM (BlackBerry) as the third largest provider of Smartphones.

The Apple iPhone already has a significant footprint in forensics investigations, going by the number of cases that appear. The iPhone has an active ethical hacking community that is engaged in research and has yielded tools to support forensics investigations. Several commercial software packages now offer iPhone support (for more details on this refer to Ref. #3, Books, Further Reading). The iPhone is a complex electronic device.

The Apple iPhone's OS, iPhone OS, is a variant of Apple's core OS, OS X. It is based on the same MACH kernel and it also shares some core elements with OS X 10.5. The iPhone comprises four layers including the core OS, the Core Services API, the Media layer and the Cocoa Touch layer. The iPhone is designed to communicate with a computer via an interface called the Apple File Communication (AFC) Protocol. This protocol is a serial port protocol that uses a framework called Mobile Device installed with iTunes (default on Apple's OS X). The protocol uses the USB Port and cable when it is connected to the computer and is responsible for things such as copying music and photos and installing firmware upgrades.

There are many technical books dedicated to the iPhone OS and the development of applications to run on iPhone. The iPhone software development kit (SDK) is free to download after registration and is recommended for anyone performing forensics analysis on the iPhone which consists of modules, chips and other electronic components from many manufacturers. Owing to the complex and varied features of the iPhone, the list of hardware is extensive. It is not possible to mention model and part numbers. Table 8.5 lists the

Table 8.5 | iPhone hardware components

<i>iPhone Function</i>	<i>Manufacturer</i>	<i>iPhone Function</i>	<i>Manufacturer</i>
Application Processor (CPU)	Samsung	Battery charger/USB controller	Linear Technology
3D graphic acceleration	Imagination Technologies	GPS	Infineon
UMTS power amplifier (PA), duplexer and transmit filter module with output power detector	TriQuint	NAND flash	Toshiba
UMTS transceiver	Infineon	Serial flash chip	SST
Baseband processor	Infineon	Accelerometer	ST Microelectronics
Baseband's support memory	Numonyx	Wi-Fi	Marvell

(Continued)

Table 8.5 | (Continued)

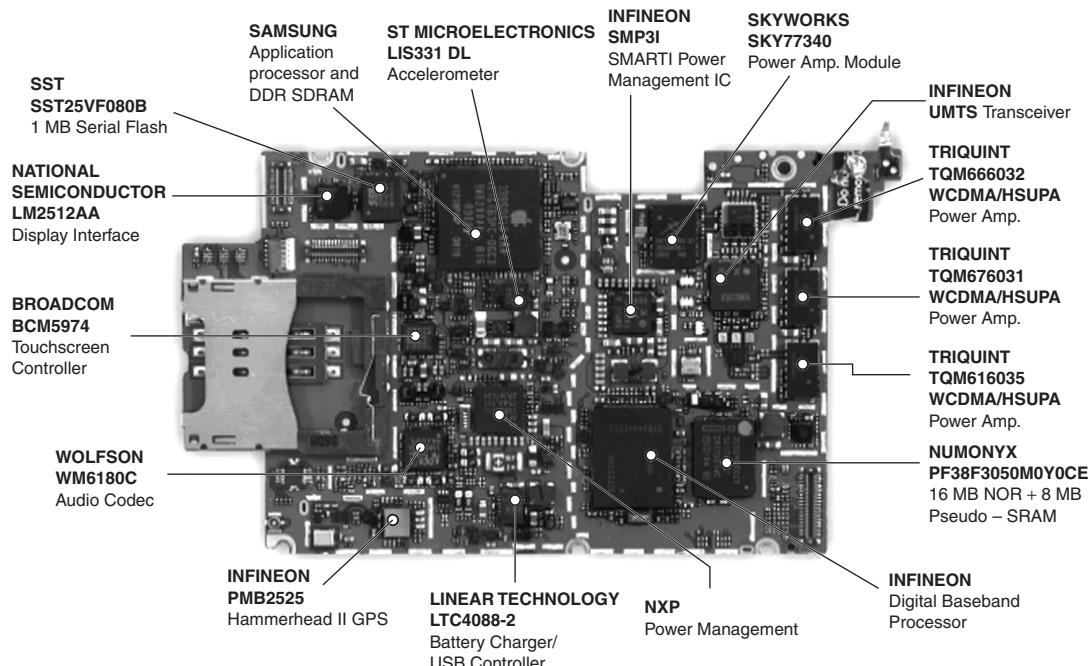
<i>iPhone Function</i>	<i>Manufacturer</i>	<i>iPhone Function</i>	<i>Manufacturer</i>
GSM/EDGE quad-band amp	Skyworks	Bluetooth	CSR
GPS, Wi-Fi and BT antenna	NXP	Audio codec	Wolfson
Communications power management	Infineon	Touchscreen controller	Broadcom
System-level power management	NXP	Link display interface	National Semiconductor
Touchscreen line driver	Texas Instruments	—	—

“function” inside an iPhone and mentions its associated manufacturer. Note that by no means this list is claimed to be exhaustive; technology keeps changing rapidly. List of iPhone OS devices can be accessed at http://en.wikipedia.org/wiki/List_of_iPhone_OS_devices (30 April 2010).

Figures 8.5 and 8.6 depict the tear-down images of iPhone presenting the top and bottom view, respectively, and various parts supplied by manufactures mentioned in Table 8.5.



We strongly recommend readers to visit the iPhone-related links mentioned in Refs #1 and #2, Video Clip, Further Reading.

**Figure 8.5 | iPhone tear-down image: top view.**

Source: <http://www.intomobile.com/2008/07/14/apple-iphone-3g-tear-down-details-chipset-components.html>

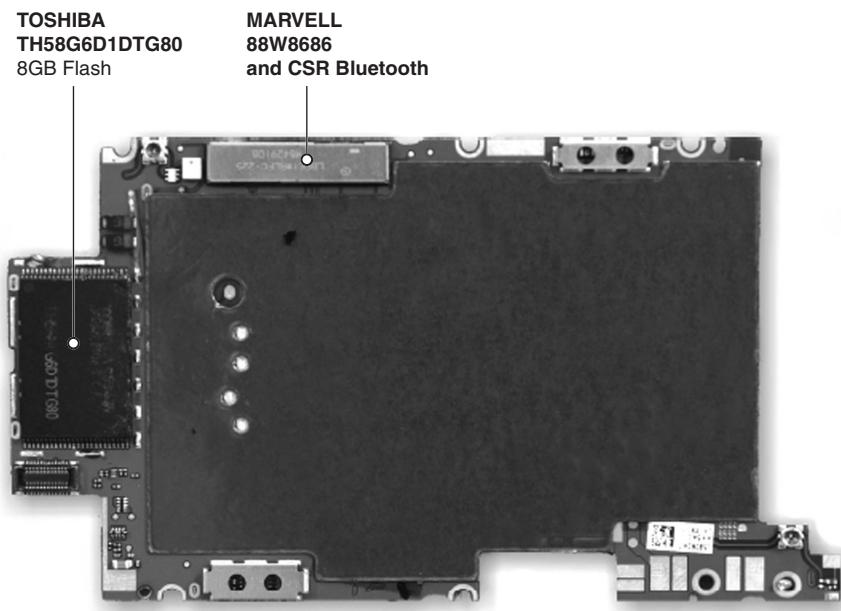


Figure 8.6 iPhone tear-down image: bottom view.

Source: <http://www.intomobile.com/2008/07/14/apple-iphone-3g-tear-down-details-chipset-components.html>

Readers who have not seen or used the Apple iPhone may be interested in knowing how to use this wonderful device. Let us now understand the forensics part of the iPhone. Paraben's device seizure is one of the leading forensics tools in the hand-held device zone and, therefore, it is presented in this section.

Like any forensics investigation, there are several approaches to use for the acquisition and analysis of information.



From evidential integrity aspect, a key aspect of any acquisition is that the procedure does not modify the source information in any manner.

In situations where it is not possible to eliminate all modifications, the analyst must keep a detailed record of the changes made and should also explain why making that change was necessary. This is especially important from the legal procedures standpoint. Forensics techniques utilized with iPhone are listed below:

1. **Acquire data directly from the iPhone:** Many analysts prefer this approach rather than recovering files from the computer. To work with this approach, that is, direct data acquisition from the iPhone, the forensics analyst needs to understand how the acquisition occurs if the iPhone is modified in any way and what is the procedure it is unable to acquire.
2. **Acquire a backup or logical copy of the iPhone file system using Apple's protocol:** With this procedure the analyst can read files from the iPhone using Apple's synchronization protocol. However, the analyst will only be able to acquire files that are explicitly synchronized by the protocol. Many key pieces of information are stored in SQLite databases and these are supported by the protocol. By querying the databases directly, the analyst, most of the times, is able to recover more information such as deleted SMS and E-Mails messages.

3. **Physical bit-by-bit copy:** With this process, a physical bit-by-bit copy of the file system gets created. The copy created with this method is similar to the approach taken in many PC forensics investigations. Although this approach has the potential for the largest amount of data recovered (including deleted files), the process is quite complicated and requires modifying the system partition of the iPhone.



Another key point of consideration for an iPhone forensics tool is how it handles an iPhone that has a pass code set.

Forensics products offer different strategies for this situation, each with its own benefits and drawbacks. However, that discussion is beyond the scope of the chapter. Paraben device seizure tool is highly recommended by forensics experts for acquiring iPhone data for forensics. Device seizure is a forensics software tool that performs acquisitions on over 2,700 hand-held devices (including phones, PDAs and GPS devices and iPhone) and runs on Microsoft Windows. The package is designed to support full acquisition and investigation process. Paraben stresses their ability to perform physical acquisition vs. logical ones as they provide the ability to recover deleted files and other important information. They have several packages that include the device seizure software and various cables for phone acquisitions. To acquire data from iPhone using device seizure, you will need to install Paraben's device seizure product. After device seizure starts, you will have to create a new case and enter basic information using the screen as shown in Fig. 8.7. Next, you will need to specify information about the examiner, that is, the person who is going to do the forensics. A screen for that is shown in Fig. 8.8.

Next, you can run the acquisition wizard or you can also import from an iPhone backup with the import wizard. The screenshot is shown in Fig. 8.9. Then you need to select how you want to acquire the iPhone

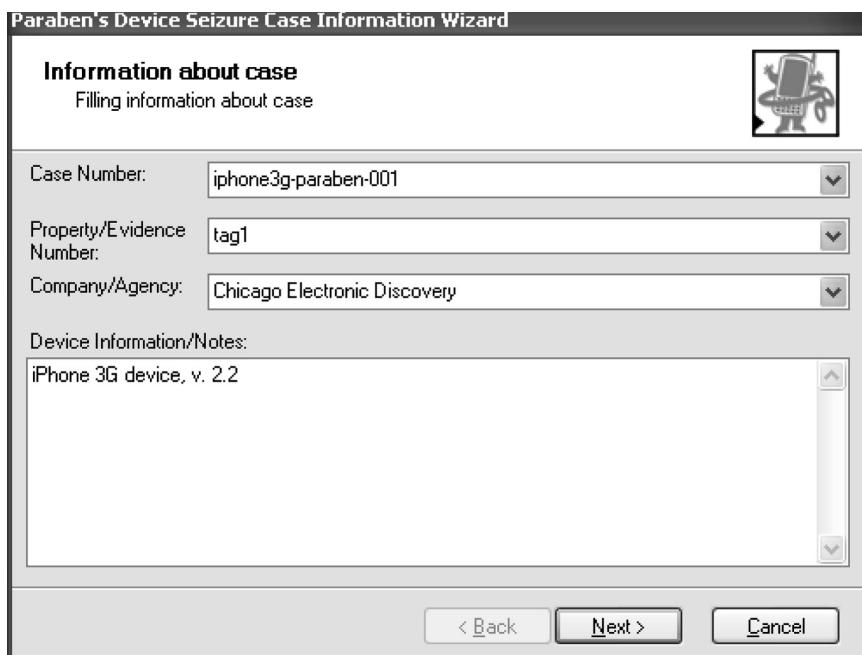


Figure 8.7 | Device information screen.

Paraben's Device Seizure Case Information Wizard

Information about the examiner
Filling Information of the Examiner



Examiner: Andrew Hoog

Address1: 3651 W CORNELIA AVE UNIT A

Address2:

Country: USA State: IL Zip: 6-618

City: CHICAGO Phone: 773-539-790 Fax:

E-mail: ahoog@chicago-ediscovery.com

Notes:

< Back Next > Cancel

Figure 8.8 | Information examiner screen.



Figure 8.9 | Device seizure wizard screen.

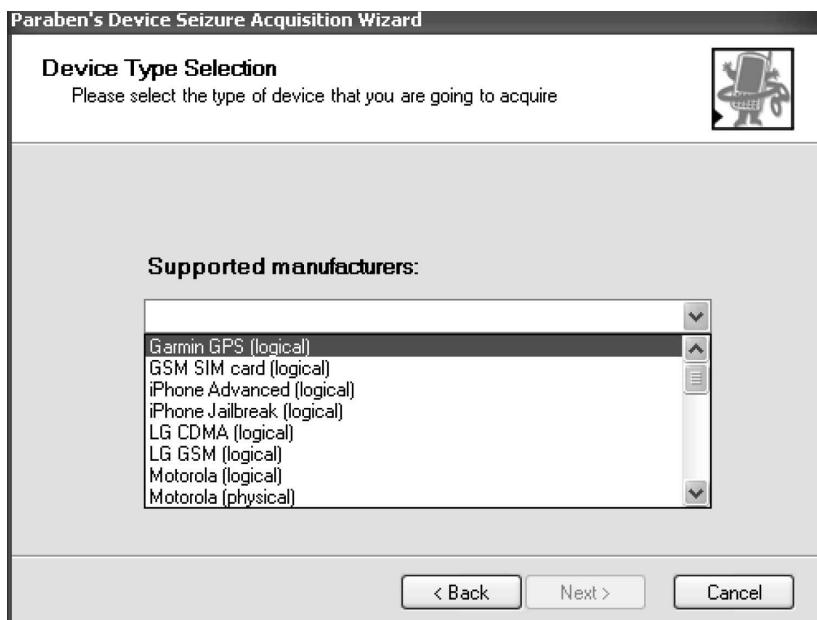


Figure 8.10 | Device selection screen.

(see the screenshot depicted in Fig. 8.10). This is where the information from Paraben's Technical Support helps. Paraben provides two methods for acquiring data from an iPhone and has named them "iPhone Advanced (logical)" and "iPhone Jailbroken Devices."^[4] It is recommended running both acquisitions against an iPhone to yield good results.

Once *device seizure* (the tool) detects the device, investigator is ready to start. Figure 8.11 shows the selection summary. Also refer to Box 8.3 and Table 8.3 for more information on hand-held devices and digital forensics.

Box 8.5 “Jailbroken” Devices!!

“Jailbreaking” is a process used with certain hand-held devices. The process allows iPad, iPhone and iPod Touch users to run any code on their devices - the code need not be the one that is authorized only by Apple. “Jailbroken” phones are vulnerable because users may disable key security features provided by Apple to get around the terms of usage agreement that they are designed to enforce. When “jailbroken,” iPhone users are able to download many applications (that were previously unavailable) through the App Store via unofficial installers such as Cydia as well as illegally pirated applications. There is indeed a problem, because, a jailbroken iPhone or iPod Touch is still able to use and update applications downloaded and purchased from Apple’s official store. It is said that 8.5% of all iPods and iPhones are jailbroken!

It should be noted that “Jailbreaking” is not same as SIM unlocking. Once SIM unlocking is completed, the mobile phone will accept any SIM without restriction, for example, the country or network operator of origin. It is a concern for Apple, because “Jailbreaking” voids Apple’s warranty on the device, although this is quickly remedied by restoring the device in iTunes. Some jailbroken phones have the potential risk of an iPhone worm. This worm was created by Ashley Towns, a 21-year-old Australian technical college student. The worm exploiting vulnerabilities in “jailbroken” iPhones is isolated both by the type of device and geography. However, it is a harbinger of threats to come against increasingly powerful Smartphone platforms.

To understand how iPhone unlocking works, you can visit the link: <http://newsblaze.com/story/20070926073901chil.nb/topstory.html> (1 May 2010).



Figure 8.11 | Summary of selections screen.

Both the iPhone Advanced and iPhone Jailbroken Devices only (called iPhone Jailbreak) methods are known to be fast, taking only a few minutes each. Next you start the “Acquisition” process (see the screenshot in Fig. 8.12).

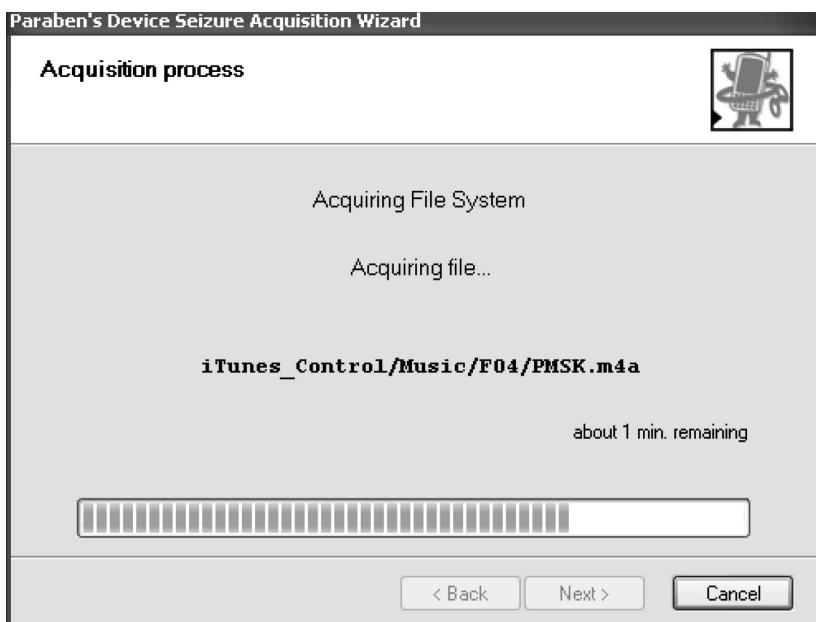


Figure 8.12 | Acquisition process screen.



In forensics parlance, “acquisition” means creating an exact physical duplicate of the original.

For benchmarking iPhone forensics toolkits available in the market, the test cases represented in Table 8.6 will be useful. Note that it is only a representative table and there could be many more possible test cases.

Other tools used for iPhone forensics in environments other than Windows XP are as follows:

1. **MacLockPick** is a valuable tool for forensics professionals, especially those who come from law enforcement background. This tool is meant to perform live forensics on Mac OS X systems. The solution uses a USB flash drive. The drive can be inserted into a suspect’s Mac OS X computer that is running (or is in “sleep” mode). By running this software, the analyst can extract forensics data

Table 8.6 | iPhone forensics: Sample list of test cases

<i>Test Case Scenario</i>	<i>Description</i>
Passwords	Determine whether the tool can find various application and network password information on the phone
SMS	Determine whether the tool can find short message service (SMS) information on the phone
Call Logs	Determine whether the tool can find call log information on the phone
E-Mail	Determine whether the tool can find E-Mail messages on the phone You can synchronize the iPhone with E-Mail applications
Contacts	Determine whether the tool can find contact information on the phone
Phone information	Determine whether the tool can report on basic phone information
Speed dials	Determine whether the tool can find speed dial information on the phone
Voicemail	Determine whether the tool can find voicemail information on the phone
Notes	Determine whether the tool can find notes information on the phone
Calendar	Determine whether the tool can find calendar information on the phone
Songs	Determine whether the tool can find music files on the phone
Pictures	Determine whether the tool can find image files on the phone
Bookmarks	Determine whether the tool can find bookmarks from the Safari web browser on the phone
Web History	Determine whether the tool can find web browser history information on the phone
Cookies	Determine whether the tool can find web browser cookie information on the phone
Google Maps	Determine whether the tool can find Google Maps information on the phone
Applications	Determine whether the tool can find application information on the phone
Configuration files	Determine whether the tool can find phone and application configuration files in the XML and Plist formats on the phone
Video	Determine whether the tool can find video information on the phone
Podcasts	Determine whether the tool can find Podcast information on the phone
VPN	Determine whether the tool can find VPN configuration information on the phone
Bluetooth	Determine whether the tool can find Bluetooth pairing information on the phone
GPS	Determine whether the tool can find GPS information on the phone
File Hashes	Determine whether the tool creates MD5 or SHA1 hashes for information on the phone
YouTube	Determine whether the tool can find YouTube video information on the phone
HTML	Determine whether the tool can find cached HTML files on the phone
Office Documents	Determine whether the tool can find Office documents (PDF, Word, Spreadsheets and PowerPoint) documents on the phone

from the Apple Keychain (a centralized location) and system settings to provide the examiner with fast access to the suspect's critical information. The added advantage is that very little interaction is required and very little trace is left behind.

2. **WOLF** is from Sixth Legion, LLC (a division of Innovative Digital Forensic Solutions) It is a forensics tool designed specifically for the iPhone. As such, it supports all iPhone models (2G and 3G) running any firmware versions. However, the software only runs on Mac OS X (10.4.11 or greater). As at the time of writing this, it is said that Windows version (called Beowulf) is to be released soon. There are a few conditions though while working with WOLF – (a) a dongle is required to run the software and (b) you must install the Code Meter framework to activate the dongle. WOLF has the ability to bypass the security pass code (iPhone, SIM or both) and it can do this bypass without jailbreaking the iPhone. This is possible provided you have access to a physical computer that the phone has been used with. WOLF also claims to be the only iPhone forensics software that can work without modifying the iPhone. This means that you can place an acquisition utility on the iPhone during acquisition to perform acquisition. WOLF acquires data from the iPhone using a logical copy of the data but it cannot recover deleted data.
3. **Cellebrite UFED Forensics System** empowers law enforcement, anti-terror and security organizations to capture critical forensics evidence from mobile phones, Smartphones and PDAs. UFED can extract vital data from various devices such as phonebook, camera pictures, videos, audio, text messages, call logs, ESN IMEI, ICCID and IMSI information. It can do this extraction from over 1,600 handset models, including Symbian, Microsoft Mobile, BlackBerry and Palm OS device. UFED analysis also includes memory dump analysis, providing access to system files and deleted messages.
4. **MDBackup Extract** is a Mac-only forensics tool from BlackBag Technologies (makers of Macintosh Forensic Suite and MacQuisition Boot Disk) that analyzes data from the iTunes mobile sync backup directory. The tool is currently in Beta version and production information is limited. As this is a Mac-only utility, you must copy the backup directory from a Windows computer to a Mac for analysis.
5. **Zdziarski's method** is unique because by using this method the examiner can perform a bit-by-bit copy of the iPhone's user partition. See Ref. #3, Books, Further Reading. Using this method, the forensics examiner can provide an MD5 sum to prove that the copy was authentic. However, there is one hitch - this ability does not exist with the standard iPhone OS and, therefore, it becomes essential to modify a read-only system partition to make this technique work. The relief is that the system partition remains completely isolated from the partition containing user data. It is intended to remain in a factory state throughout the life of the iPhone. With this isolation facility, it becomes an ideal and forensically sound location to perform the required payload installation without violating user data.

There are many challenges in iPhone forensics as iPhones are becoming increasingly important in corporate investigations, civil and criminal cases, and even marital disputes. Much can be recovered through iPhone forensics – text (SMS) messages, voice mails, call logs, GPS coordinates, websites visited, etc. and today's Smartphones can make or break a case. For forensics of iPhones, not many experts are available. iPhone platform is proprietary, relatively new and it is characterized by frequent changes. Table 8.5 shows the hardware complexity of the iPhone which is only one dimension of the complexity involved. One can imagine how complex the software must be. There is a link provided to the suite of iPhone Forensics Software Solutions.^[5] Leading books, on iPhone forensics topics, are also indicated in Refs. #3 and #6, Books, Further Reading.

8.3.7 Challenges in Forensics of the Digital Images and Still Camera

Forensics image processing, over the years, has expanded to more areas, including questioned document examination; footwear, tire impression and tool mark examination; blood spatter evidence; bullet striation and primer mark examination; etc. As technology progressed, video analysis moved to digital realm, resulting into new tools and the need for experts with specialized knowledge in image processing. Times have changed today's image analysis and enhancement is quite different than what was seen in the early 1990s. Now, we can undertake quite a bit of non-destructive processes using adjustment layers, we can localize enhancements with layer masks and we can also utilize features of various digital image processing tools to extract a fingerprint from a background or find detail that was not visible to the naked eye. Image rendering graphics capabilities allow us to apply a Fast Fourier Transform to eliminate patterned backgrounds, apply deconvolution to correct motion blur or poor focus and utilize frame averaging to eliminate noise from a sequence of images. There are software tools available for correcting lens distortion. There is a heavy implication of all this – the crime case investigators must become very good at digital image forensics or digital camera forensics because now digital cameras are ubiquitous compared to the cellular mobile phones.

During a forensics investigation, the experts may come across a number of digital photographs; for example, law enforcement examining computers for intellectual property disputes involving proprietary digital images, or file recovery for individuals who have lost personal photos due to accidental deletion or electronic media corruption, image evidences of child pornography, etc. Digital image forensics technique is used to distinguish images captured by a digital camera from computer-generated images. Digital rights management, locating steganographic images, etc. are some more technical examples. Steganography in forensics context was mentioned in Section 7.12, Chapter 7. The file extension .jpg is most commonly referred to as the JPEG file format – “a lossy compression method that takes advantage of the limitation of the human eye.” Steganographic techniques used by cybercriminals are often based on this – refer to discussion in Chapter 7, especially Box 7.15.



Digital cameras generally use JPEG compression to encode images and different manufacturers typically configure their devices with different compression levels and parameters.

Some examples of digital photographs and images, used for evidential purposes, are shown in Fig. 8.13. The integrity of a digital image is paramount in the forensics field. Courts make decisions affecting an individual's liberty based, in part, on images presented as evidence.

As it is frequently necessary to make corrections and adjustments to images (e.g., to separate one type of cell from another or to enhance a fingerprint), it is important to maintain the integrity of images from capture through final usage.

With modern image processing technologies and photo processing software tools available, changing/manipulating digital images is no more difficult. Due to the migration from traditional photography to digital photography, forensic institutions and wider law enforcement agencies have concerns regarding security, integrity and continuity of digital images. Interestingly, many of the questions raised by the introduction of digital cameras were not always necessarily addressed while photography was in use, because “historic” practices had grown up around its use and had not been scrutinized as closely as digital is now. It would be interesting to imagine what would have happened if digital was replaced by photography!

There are two main interests in “image forensics,” namely, source identification and forgery detection. A major concern over digital images has been the fact that the “original” or “master” image is not so

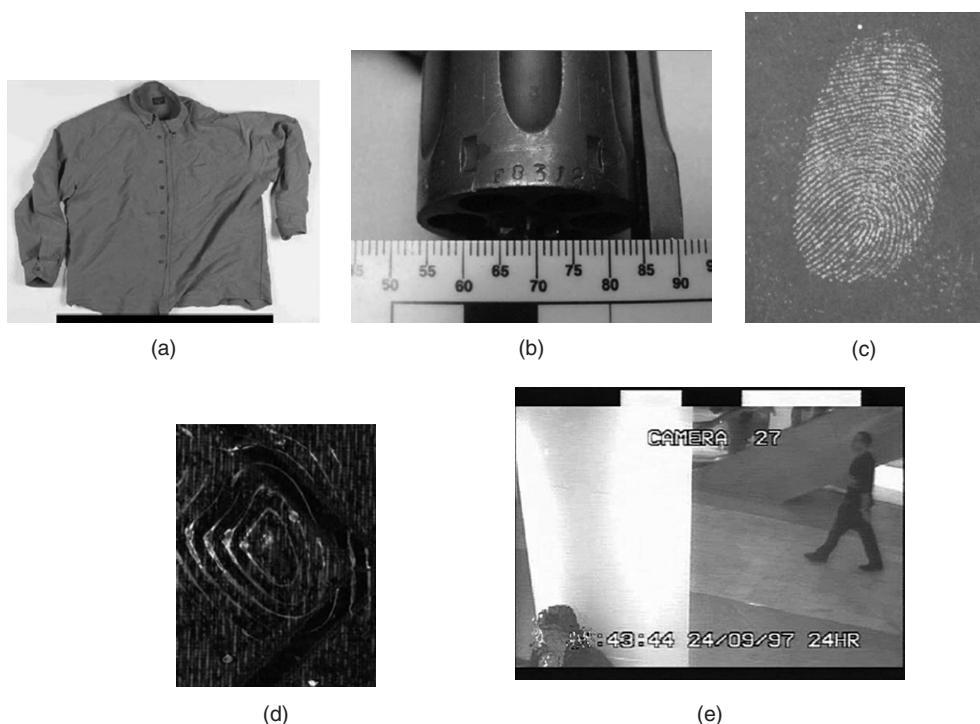


Figure 8.13 Digital photographs and images examples. (a) Type of note taking image used as an illustration of the shirt examined, (b) record image of a firearm which is generally used for court purposes, (c) typical image (finger mark) used for Biometric comparison, (d) intelligence image in which shoe-mark image provides information about the make and model of the shoe, (e) a CCTV image.

easily defined; there is no digital “negative” that neatly corresponds with a photographic negative. This lack of a physical entity has led to debates over what is the “original” image, which in turn has led to a lack of clarity over what needs to be retained as best evidence for the courts. In some cases, the storage media (e.g., CDROM, Flashcard, etc.) is retained because it represents the first permanent record of the image. Others contemplate the storage of an identical “copy” of the first permanently recorded image where this is more practical and one can rely upon appropriate operating procedures/technology to ensure an identical (bit-for-bit) and reliable copy is produced.

Storage devices are getting miniaturized and are available in a hidden way and as combined miniature digital cameras too – refer to Fig. 7.3 in Chapter 7. The advances in digital imaging technologies present new issues and challenges concerning the integrity and authenticity of digital images. Digital images can now be easily created, edited and manipulated without leaving any obvious traces of such operations. For example, take a look at the images in Figs. 8.14 and 8.15.

In Fig. 8.14, the top image is uncorrected and the bottom image has been given a “level adjustment” layer with a layer mask, so that the background could be lightened, while keeping the foreground from becoming too bright. These manipulation capabilities undermine the credibility of digital images in all aspects. “Channel Mixer” tool is one of the most powerful tools used for image enhancement tasks. This tool makes it possible to combine the channels of a color space to be mixed in different percentages to affect the tonal



Figure 8.14 | Digital image adjustment example.

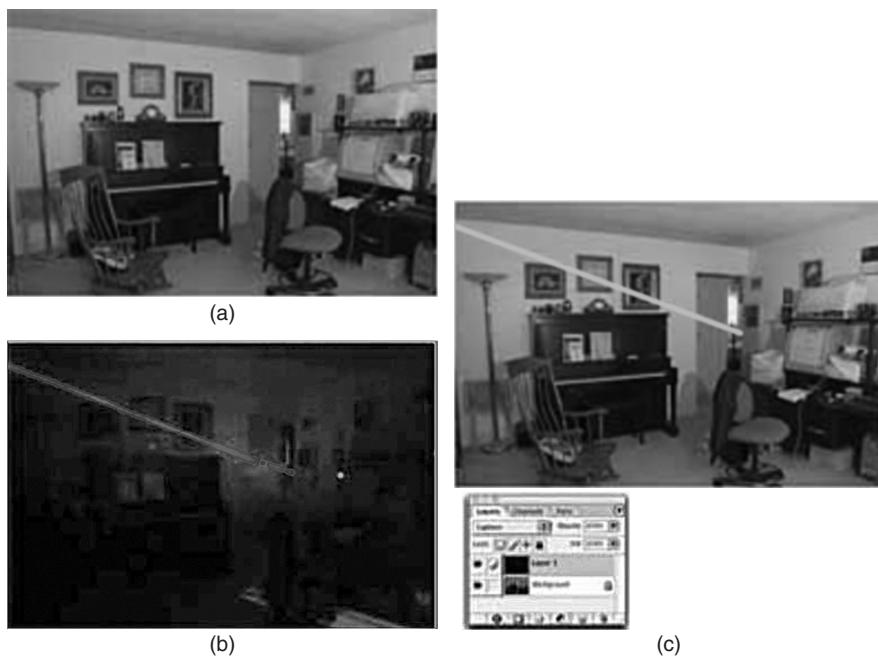


Figure 8.15 | Bullet trajectory mapping example.

contrast between various colors. In forensics analysis work, this works out to be a great advantage because the analyst can extract a fingerprint from a busy background. The analyst can also isolate an endorsement signature from the bank or store imprinting, or even recover “invisible” writing from stolen checks that may have got bleached and rewritten.

In Fig. 8.15(a) a living room is photographed during daylight using flash. Figure 8.15(b) shows a bullet trajectory; it is prepared by using a laser pointer with no room illumination. Figure 8.15(c) combines the two images resulting in the image of the well-lit room with the trajectory. This has been achieved by using the “lighten mode” in Photoshop’s layers.



In courts, there are often situations wherein digital photographs are produced as evidence. Digital image forensics is an emerging research field aiming at determining the origin and potential authenticity of a digital image.

Being able to store an audit trail in the file’s metadata has benefitted forensics. There is no court requirement for having an audit trail, but it is a key feature in validating that good techniques are used and makes it possible to easily repeat most enhancements. The Log, containing all the history, can be invoked through the “General Preferences” pane in Photoshop. Recording metadata is very crucial – once recorded, the metadata can be viewed by choosing history from the File Info dialog box or in the Metadata tab in Photoshop’s File Browser.



A fundamental problem that digital image forensics techniques attempt to solve is the identification of the source of a digital image.

It is important to be able to determine the means by which a digital image has been created, for example, digital camera, scanner, generative algorithms, etc. Image source identification may include one of the following approaches:

1. Verifying and evaluating the image statistics that are inherent to real-life scenarios and objects;
2. detecting, classifying and measuring the qualities of spatial structures (i.e., color, texture and edge structures) in an image;
3. identifying signatures to detect traces of certain types of operations used in image generation process by possible sources.

Identifying whether a given image is a depiction of a real-life occurrence (and objects) or a fictitious realization forms a specific interest for digital forensics investigators.



The challenge is the ability to distinguish digital images generated by a digital camera from the ones generated by a computer graphics rendering tool.

Generally, image acquisition in a digital camera includes many common processing stages (regardless of the specific digital camera used in capturing the image) leaving a unique signature in certain properties of the

resulting image which may not necessarily be present in synthetically generated images. The responsibility for any forensics image interpretation within different establishments is mixed. In some instances there are dedicated imaging experts who deal with the technical aspects of the images and also the interpretation of events or objects in the image. Other organizations draw on a pool of experts from different forensics areas to interpret and address different aspects in the case. This combined approach prevents experts from straying from their area of expertise.

For image processing, emerging best practice suggests that a bit-for-bit copy of the “original” or “master” image is produced and this becomes a “working copy.” It is the working copy that is used for subsequent processing or analysis. An audit trail is used to track changes made to the image. The audit trail needs to be of sufficient detail to replicate the processing carried out. The processed image may become an item or evidence within the case and requires standard approach to be taken with such entities. In particular, backup and archiving of images are required and currently, a write once/read many (WORM) type medium is the preferred choice. Storage area networks are being thought of as a solution. Mirroring data storage as a contingency for data loss is an important consideration.

8.3.8 Forensics of the BlackBerry Wireless Device

“BlackBerry” was mentioned in many sections of this chapter; let us understand the “BlackBerry” – especially, how it is different from a “PDA.”



The BlackBerry, which is also known as a RIM device, was developed by Canadian company “Research In Motion” (RIM).

The first BlackBerry device was introduced in 1999 – it was meant to be a two-way pager. In 2002, the more commonly known Smartphone BlackBerry was released. This device supports push E-Mail, mobile telephone, text messaging, Internet faxing, web browsing and other wireless information services. The BlackBerry devices are a classic example of a “convergent device,” that is, multiple technologies converging in a single device and that presents a forensics challenge.

The BlackBerry device is equipped with the Research In Motion (RIM) software implementation of proprietary wireless-oriented protocols; furthermore, the device is supported by the RIM BlackBerry Message Center. As for the hardware, the RIM device is designed around an Intel 32-bit i386 processor, a low-power-embedded version of the same processor that used to power a desktop PC. Each unit has 512 KB of static RAM (SRAM) and 4 or 5 MB of Flash RAM, depending on the model. The RIM’s Static Random Access Memory (SRAM) is analogous to the RAM on a desktop and the Flash memory is the “disk space” used to store the OS, applications and the file system. The RIM’s OS is a single executable named PAGER. EXE and the applications are dynamic link libraries (DLLs).

The BlackBerry (RIM) device shares similarities to the PDA devices we addressed earlier.



The BlackBerry (RIM) device is always-ON and participates in some form of wireless push technology. As a result of this, the BlackBerry (RIM) does not require some form of desktop synchronization like the PDA does.

This unique feature of the BlackBerry (RIM) device, however, adds a different dimension to the process of forensics examination. In essence this portability aspect of the BlackBerry can work to the forensics examiner's greatest convenience. The BlackBerry (RIM) device has an integrated wireless modem allowing the device to communicate over the BellSouth Intelligent Wireless Network.^[6] The protocol, used by BlackBerry (RIM) device, is known as the "BlackBerry Serial Protocol." The data communicated between the BlackBerry (RIM) hand-held unit and the desktop software is backed up, restored and synchronized using this protocol. BlackBerry Serial Protocol consists of simple packets and single byte return codes. The device uses a strong encryption scheme to safeguard confidentiality and authenticity of data. Data is secured through encryption while in transit between the enterprise server and the device itself.

From a forensics perspective, the RIM device shares the same evidentiary value as any other PDA. The forensics investigator would suspect almost the entire set of file systems and therefore, a "delete" action by no means is to be taken as total removal of data on the device. However, as already mentioned, the RIM is always-ON; wireless push technology adds a unique dimension to forensics examination. Changing and updating data no longer requires desktop synchronization. In fact, a RIM device does not need a cradle or desktop connection. The more time a hand-held device spends with its owner, the greater the chance that it will more accurately reflect and tell a story about that person! Thus, RIM's currently unsurpassed portability is the greatest ally for the forensics examiner.

Now, let us understand the care to be taken during "acquisition" phase in BlackBerry forensics.

1. **If the RIM is OFF, leave it OFF:** If the unit is OFF at the time of acquisition, the investigator needs to take the unit to a shielded location before attempting to switch the unit ON. If a shielded location is not readily available, a safe room should be used to block the signal well enough to prevent the data push. One important thing to consider is having a unit available that can be used to walk the network and area to test the coverage, looking for weak coverage areas to use.
2. **If the RIM is ON, turn the radio OFF:** If the BlackBerry device under examination is in the "ON" state then as mentioned above, you need to take the device to a secure location and disable or turn OFF the radio before beginning the forensics examination.
3. **If the RIM is password protected, get the password:** When it comes to password protection one important thing to consider is the fact that the password itself is not stored on the device, the only thing that is stored on the device is a hashing of the plain text password. This storage is similar to the storage used by the majority of OS out there.

As the BlackBerry is an "always ON," push messaging device, information can be pushed to the unit through its radio antenna at any time, potentially overwriting previously "deleted" data. Without warning, applications such as the E-Mail client, instant messaging, wireless calendar and any number of third-party applications may receive information which makes the forensics investigator's attempts to obtain an unaltered file system much more difficult. In order to preserve the unit, turn the radio OFF. There are good reasons why the entire unit should not be turned OFF:

1. The BlackBerry is not really "OFF" unless power is removed for an extended period of time or the unit is placed in data storage mode. Only the display, keyboard and radio are shutdown when using the graphic user interface (GUI) to turn OFF the unit.
2. When the unit is again turned ON from an "OFF" or true powered down state, queued items may be pushed to the unit before there is a chance to turn the radio OFF.
3. A software program might be installed on the unit that can accept remote commands via E-Mail. Under certain circumstances the original owner may prefer an investigator not view the information on a BlackBerry, and use this software to alter or delete information. Of course, this depends on the circumstances under which the forensics investigation is taking place.

As mentioned before if the unit is OFF at the time of acquisition, take it to a shielded location to turn it ON and immediately shutdown the radio before examination. A file cabinet or safe should block the signal well enough to provide time to work with the radio. Sometimes an interior room will do. It is ideal to have a unit on each network available to test local coverage (or lack thereof) for a safe location. The BlackBerry does not rely on an external power source, therefore, the examiner must ensure that the unit does not power down as the result of a dead battery before the examination is complete. The specific care to be taken depends on which model of BlackBerry is involved. However that discussion is beyond the scope of this chapter. If the AA battery is changed fast, the charge stored in the unit will keep it running. It will take too long and the unit will enter the radio/LCD/screen-off mode and eventually enter a full power-down mode. The radio/LCD/screen-off mode will cause changes to the system logs. The more destructive full power-down mode will cause a reset at startup wiping out most of the logs and initiating a system cleanup. A system cleanup has the forensically undesired effect of reclaiming unallocated (previously deleted) files by wiping and reorganizing sections of the file system. Note the following:



Completely powering OFF the RIM BlackBerry device will wipe data from the SRAM. Logs of interest, stored in SRAM, will not survive a full power-down.

The tricky situation in investigating the RIM, using available tools, is that a file system snapshot ends in the same destructive reset that will wipe some of the logs, but investigating the logs could quite probably cause unwanted changes to the file system as well. Forensics examiner needs to be familiar with the contents of the logs and their applicability case-by-case – for example, as mentioned earlier, the password needs to be obtained if the RIM is password protected. RIM provided software should be used because it will not circumvent password protection. As mentioned earlier, the password itself is not stored on the unit; rather an SHA-1 hash of the password is stored and compared to a hash of what is entered. The examiner only has the opportunity to guess 10 times before a file system wipe occurs to protect the data. This wipe will destroy all non-OS files. No third-party software is available to circumvent the password protection. A direct-to-hardware solution will be required if the password is not available.

Now let us understand the “evidence collection” phase in BlackBerry forensics examination. To collect “evidence from the BlackBerry,” traditional forensics methods need to be violated in the sense that the investigator needs to record logs kept on the unit because they will be wiped after an image is taken. There are several different log files that can be used to collect evidence from:

1. **Radio Status:** This log lets us enumerate the state of the devices’ radio functions.
2. **Roam and Radio:** This log has a buffer of up to 16 entries; usually records information concerning the tower, channel, etc.; and will not survive a reset.

Once the log information is extracted and enumerated then the image will be taken. If you do not require or need the log information then the image can be acquired immediately.



For the forensics examiner, the logs reviewed by using BlackBerry unit’s “control functions” are very important.

The BlackBerry unit has many control functions (see Figs. 8.16–8.19). In Fig. 8.16(a) the first function is “Mobitex2 Radio Status.” This function provides information on the Radio Status, Roam and Radio Transmit or Receive and Profile String. Figure 8.16(b) denotes the second control function – “Device Status.”

As the name implies, the “device status” function [Fig. 8.16(b)] provides information for battery type, load, status and temperature. The Mobitex2 Radio Status screen provides access to the four following logs:

1. **Radio Status:** It enumerates the state of radio functions.
2. **Roam and Radio:** It records base/area (tower) and Roam (channel) information for duration of up to 99 hours per base/area/channel. This log wraps at 16 entries and will not survive a reset. A blank entry represents a radio-off state.
3. **Transmit/Receive:** It records TxRx, gateway MAN addresses, type and size of the data transmitted, and both network and hand-held date stamps per transmission.
4. **Profile String:** This is a recorded negotiation with the last utilized radio tower.

From forensics perspective, the *Roam and Radio log* is most interesting. A call to a radio network provider or on-location testing using a test RIM will provide the physical location that corresponds to each base/area. The investigator may be interested, for example, to know that the RIM in question has been to Hyderabad, Andhra Pradesh (a state in India) say, in the last 3 days. Each entry is a record of location at a single base/area location for up to 99 hours. The counter is always running, even when the radio is turned OFF, and so these values must be recorded as soon as possible to avoid log overwrites.

(a) Mobitex2 Radio Status

MAN: 1500000000_TrafNum 0.0	1. Radio status
Base 1 Area 2 Rssi -83dBm	2. Roam and radio (locator)
Ch <0100, 3220> 930.2500MHz	
Net B433 GrpLst	
TxPow 0dBm	
FF 0/0	3. Transmit receive
OnRmTmTmRmCg	4. Profile string

(b) Device status

Battery: 100% 4.00 V	1. Type, load, status and temp
Build: 0532 2.1.23 Feb 26 2001	2. Memory allocation information
Free Mem: 285284 bytes	3. Port status
Comm Port 0 Closed	
Comm Port 1 Closed	
File system	4. File system allocation information
WatchPuppy	5. CPU WatchPuppy

Figure 8.16 BlackBerry unit's control functions – set 1. (a) Radio status control and (b) device status control.

Source: June 2002 paper *Forensic Examination of a RIM (BlackBerry) Wireless Device*. Visit <http://www.rh-law.com/ediscovery/Blackberry.pdf>

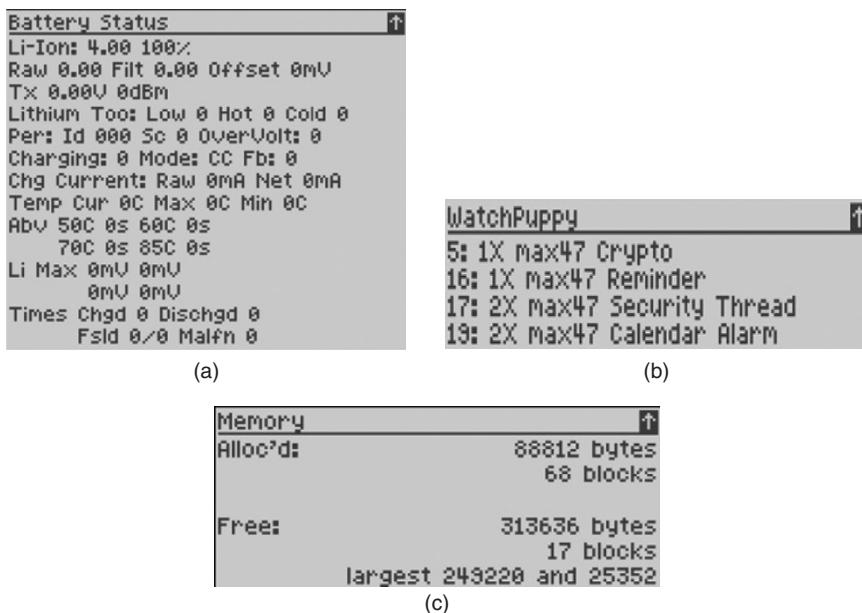


Figure 8.17 BlackBerry unit's control functions – set 2. (a) Battery status, (b) CPU WatchPuppy and (c) file memory status.

Source: June 2002 paper *Forensic Examination of a RIM (BlackBerry) Wireless Device*. It can be accessed at <http://www.rh-law.com/ediscovery/Blackberry.pdf>.

There are also the other control functions [refer to Figs. 8.17(a), (b) and (c)]. They are “battery status,” CPU “WatchPuppy” and memory allocation. The control function “Free Mem” [see Fig. 8.17(c)] provides information on memory allocation. *Battery Status* [see Fig. 8.17(a)] provides information on battery type, load, status and even temperature. The CPU WatchPuppy [see Fig. 8.17(b)] logs an entry when an application uses the CPU beyond a predetermined threshold. WatchPuppy kills processes that do not release the CPU. *Free Mem* [see Fig. 8.17(c)] provides memory allocation information including the largest free blocks. This value should be watched to prove that the unit is cleaning up the file system during a reset. The other useful control information provided by the BlackBerry unit are common port, file system [refer to Figs. 8.18(a) and (b)] and OTA status, halt and reset [see Figs. 8.19(a) and (b)]. The OTA summarizes the last items synchronized via wireless calendaring on 32 lines and provides access to debugging information (see Fig. 8.19). The log can be E-Mailed from the OTA status menu; however, this is not advised as it will result in data being written to the file system.

Pressing “R” or waiting a few seconds will cause a reset [see Fig. 8.19(b)]. This is analogous to using a paperclip to trip the reset button on the back of the unit! A reset will cause the unit to re-read the file system and can trigger a file system cleanup. It should suffice to state that during a cleanup, items marked as deleted will be irrecoverably wiped and a basic “defragment” procedure can occur. It appears also that checksums are used to pinpoint bad Flash RAM areas. The purpose of a cleanup is to provide the largest blocks of free space as far as possible for future use. However, forensics investigator will hope to avoid this because it is dangerous to get data overwritten as it will mean possible impact on the evidence being looked for.



During a forensics examination of a BlackBerry (RIM) device, “imaging and profiling” needs to be conducted.

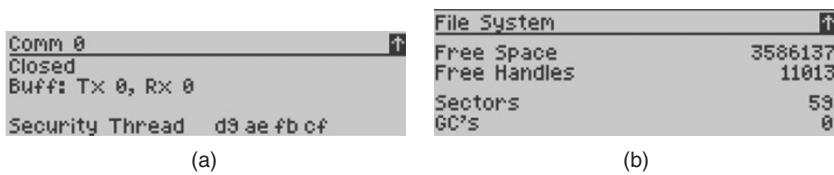


Figure 8.18 shows two screenshots of BlackBerry control functions. (a) Common port status: Comm 0, Closed, Buff: Tx 0, Rx 0, Security Thread d9 ae fb cf. (b) File System status: Free Space 3586137, Free Handles 11013, Sectors 59, GC's 0.

File System ↑	
Free Space	3586137
Free Handles	11013
Sectors	59
GC's	0

Figure 8.18 | BlackBerry unit's control functions – set 3. (a) Common port and (b) file system.

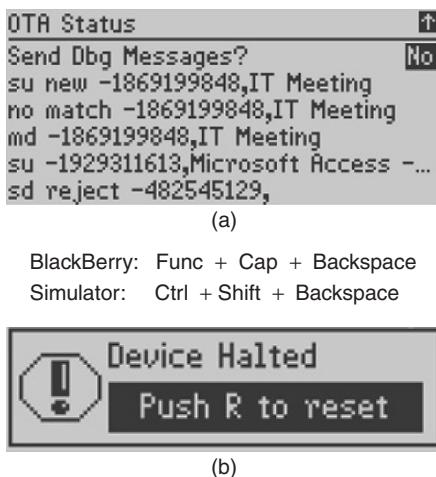


Figure 8.19 | BlackBerry unit's control functions – set 4. (a) OTA status function and (b) halt and reset status function.

This is accomplished by extracting the logs from a developed image; acquiring an image of a bit-by-bit backup is done using the BlackBerry (RIM) SDK. The SDK utility dumps the contents of the Flash RAM into a file. Once the Flash RAM is dumped, it can be examined and reviewed using traditional methods with your favorite hex editor or other tool. In addition to reviewing the evidence with traditional methods, you can use the simulator from the SDK to match the network and model of the investigated unit.

As for the forensics tools, the “BlackBerry Software Development Kit” currently contains the best tools for examining a RIM. In that sense alone they can be considered forensics. Certainly, an imaging tool that results in a reset leaves something to be desired! The kit can be downloaded by filling out a web form at the site www.BlackBerry.net. You need to install it, view the contents of the subdirectories and read through the help files before starting. The applications used to examine the BlackBerry unit are the Simulator (Simulator.exe and OSLoader.exe) and the Program Loader (programmer.exe).

8.4 Toolkits for Hand-Held Device Forensics

So far, we have been through the forensics aspects of PDAs, Smartphones, cell phones, printers, scanners, iPhones BlackBerrys and digital images/digital cameras. In this section, we provide an overview of tools available in the market. It is by no means authors' intention to promote these products. Information about

forensics toolkits is provided here only as a general information for readers' awareness. The purpose is only to emphasize the point that hand-held devices store personal information, voice calls and contact information that may provide digital evidence during an investigation. Therefore, forensics examiners need to follow clear, well-defined methodologies and procedures for proper retrieval and speedy examination of information present on the device.

Acquisition of data from a hand-held device is carried out in the following two ways:

1. **Physical acquisition:** In this particular type of acquisition, an exact copy bit-by-bit is collected of the entire physical storage which can be either a RAM chip or a disk drive.
2. **Logical acquisition:** This is an exact copy bit-by-bit of the logical storage such as file and directories, involved residing on a logical store which could be several disk drives.

Forensics examiners prefer physical acquisition much more than logical acquisition because they find it more advantageous. With physical acquisition, examiners can look at deleted files and other small remaining pieces of data much more closely. Such data can be missed out while carrying a logical acquisition. Another reason why physical acquisition is more preferred compared to logical acquisition is that physical device images can easily be imported in a different forensics toolkit for examination and reporting. Yet, logical acquisition has an advantage in providing a more natural and readable organization of the data acquired. Both methods are practiced during forensics acquisition and analysis of Palm OS.

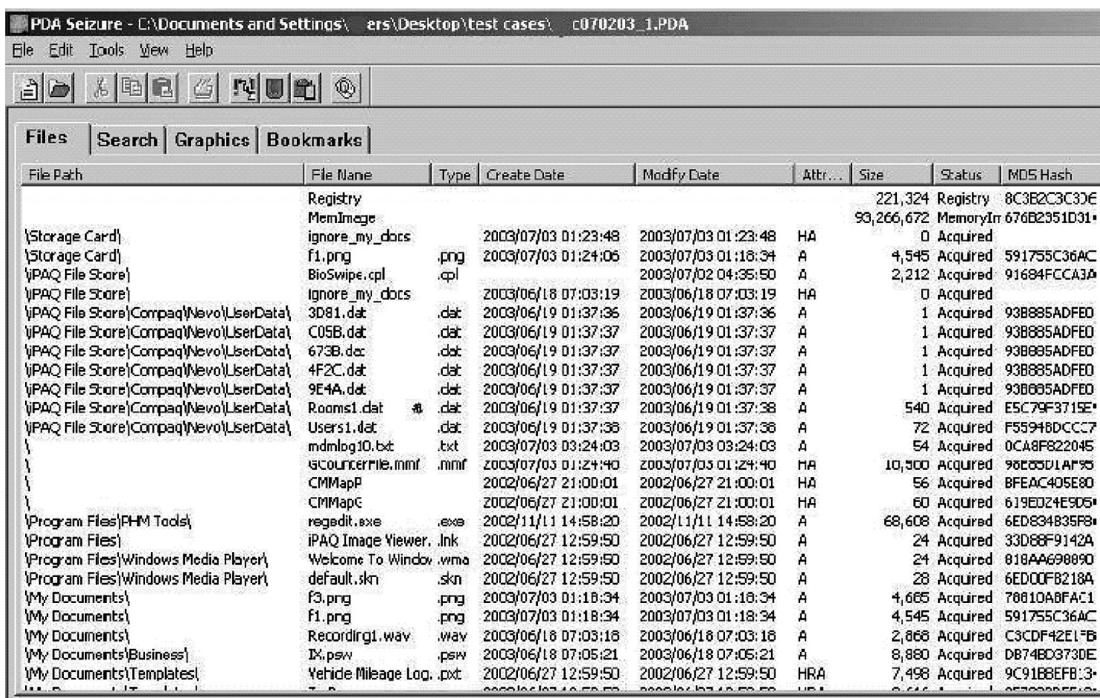
Now let us take a quick view of various tools available in the market. In Chapter 7, there was a mention about EnCase which is one of the well-known forensics tools as well as other tools too. We begin this tool overview section with tools available for PDA forensics (*EnCase*, *PDA Seizure*, *PDD*) and then describe the tools available for cell phone forensics (*Cell Seizure*, *MOBILedit!*, *ForensicSIM*, *Forensic Card Reader*). Summary of these tools is provided in Tables 8.3 and 8.4.

8.4.1 EnCase

EnCase is a popular software toolkit for hand-held device forensics. Its features support many features: analytical tools, suspect media acquisition, data capture, documentation and search features. Note, however, that EnCase does not support Pocket PC devices, although it is a very familiar tool for PCs and Palm OS devices. A complete physical bit-stream image of Palm OS devices is created and this bit-stream image is checked with the already obtained existing cyclical redundancy checksum (CRC) values. This process yields an EnCase evidence file which is created as a read-only file. From here, the software rebuilds the file structure using the logical data in the bit-stream image. The forensics examiner can then look over the device content to trace any evidence without the original data being getting manipulated. EnCase includes features such as bookmarking and reporting. Bookmarking allows files, folders or sections of a file to be highlighted and saved for later reference. Each case is bookmarked and saved in case files. Any data can be bookmarked for future reference. Forensics examiners find the reporting feature of EnCase very useful because using that feature, they can then search for information of one file, two files, multiple files, all the files in the case, etc. The examiner can also obtain a report of the entire case file that is created.

8.4.2 Device Seizure and PDA Seizure

These are two famous tools from Paraben. Paraben's device seizure is one of the many products used for viewing cell phone data. This tool was mentioned in Tables 8.3 and 8.4. Figure 8.20 illustrates an example of data acquisition through a PDA seizure toolkit. It is a forensics software toolkit to obtain and examine the data on



The screenshot shows the PDA Seizure application window. At the top, there's a menu bar with File, Edit, Tools, View, Help. Below the menu is a toolbar with icons for file operations like Open, Save, Print, and Export. The main area has tabs for Files, Search, Graphics, and Bookmarks, with Files selected. A table lists files with columns for File Path, File Name, Type, Create Date, Modify Date, Attr., Size, Status, and MD5 Hash. The table contains numerous entries, mostly from a 'User Data' folder, including files like 'ignore_my_docs', 'f1.png', 'Bioswipe.cpl', etc.

File Path	File Name	Type	Create Date	Modify Date	Attr...	Size	Status	MD5 Hash
\Storage Card\	Registry					221,324	Registry	8C382C3C3D6
\Storage Card\	MemImage					93,266,672	MemoryIn	676B2351D31*
\PAQ File Store\	ignore_my_docs	.png	2003/07/03 01:23:48	2003/07/03 01:23:48	HA	0	Acquired	
\PAQ File Store\	f1.png	.png	2003/07/03 01:24:05	2003/07/03 01:16:34	A	4,545	Acquired	591755C36AC
\PAQ File Store\	Bioswipe.cpl	.cpl		2003/07/02 04:35:50	A	2,212	Acquired	91684FCCA3A
\PAQ File Store\	Ignore_my_docs		2003/06/18 07:03:19	2003/06/18 07:03:19	HA	0	Acquired	
\PAQ File Store\Compaq\Nevo\ UserData\	3081.dat	.dat	2003/06/19 01:37:36	2003/06/19 01:37:36	A	1	Acquired	93B885ADF0
\PAQ File Store\Compaq\Nevo\ UserData\	C05B.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADF0
\PAQ File Store\Compaq\Nevo\ UserData\	673B.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADF0
\PAQ File Store\Compaq\Nevo\ UserData\	4F2C.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADF0
\PAQ File Store\Compaq\Nevo\ UserData\	9E4A.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADF0
\PAQ File Store\Compaq\Nevo\ UserData\	Rooms1.dat	*.dat	2003/06/19 01:37:37	2003/06/19 01:37:38	A	540	Acquired	F55948DCCC7
\PAQ File Store\Compaq\Nevo\ UserData\	Users1.dat	.dat	2003/06/19 01:37:36	2003/06/19 01:37:36	A	72	Acquired	
\PAQ File Store\Compaq\Nevo\ UserData\	mdmlog10.txt	.txt	2003/07/03 03:24:03	2003/07/03 03:24:03	A	54	Acquired	0CA8FB822045
\	gcounterm.mif	.mif	2003/07/03 01:24:40	2003/07/03 01:24:40	HA	10,500	Acquired	98E050ULAP93
\	CMMapP		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	56	Acquired	BFEAC405E0
\	CMMapP		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	60	Acquired	619ED24E9D9*
\Program Files\PHM Tools\	regedit.exe	.exe	2002/11/11 14:58:20	2002/11/11 14:58:20	A	68,608	Acquired	6ED834835FB*
\Program Files\	iPAQ Image Viewer.lnk		2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	33D88F9142A
\Program Files\Windows Media Player\	Welcome To Window.wma	.wma	2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	818AA698090
\Program Files\Windows Media Player\	default.skn	.skin	2002/06/27 12:59:50	2002/06/27 12:59:50	A	28	Acquired	6ED00FB2184
\My Documents\	f3.png	.png	2003/07/03 01:16:34	2003/07/03 01:16:34	A	4,665	Acquired	76010ABFA1
\My Documents\	f1.png	.png	2003/07/03 01:18:34	2003/07/03 01:18:34	A	4,545	Acquired	591755C36AC
\My Documents\	Recording1.wav	.wav	2003/06/18 07:03:18	2003/06/18 07:03:18	A	2,868	Acquired	C3CDF42EL*B
\My Documents\Business\	IX.psw	.psw	2003/06/18 07:05:21	2003/06/18 07:05:21	A	8,880	Acquired	DB74B0373DE
\My Documents\Templates\	Vehicle Mileage Log.txt	.txt	2002/06/27 12:59:50	2002/06/27 12:59:50	HRA	7,498	Acquired	9C91B8EFB13-
\	200206180710125752		200206180710125752	200206180710125752	HA	0	Acquired	972002055555

Figure 8.20 Example – PDA data acquired using a PDA seizure toolkit.

Source: http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/04_Sansurooah%20An%20overview%20and%20examination%20of%20digital%20PDA%20devices%20under%20forensics%20toolkits%20Camera%20Ready%20Paper.pdf

PDAs. A free trial of this tool (Paraben's PDA Seizure 3.0.3.86) can be taken by visiting the link <http://www.softpedia.com/get/System/Back-Up-and-Recovery/PDA-Seizure.shtml>. PDA Seizure tool can only produce a forensics image of Palm OS and Pocket PC devices. The “PDA Seizure” searches acquired files for data and generates a report of the findings. Similar to EnCase, PDA Seizure also includes the capability to bookmark and organize information. The graphics library is useful because it provides the functionality of automatic collection of images according to their file extensions. Data can only be acquired from the Palm OS device when in console mode. The logical data can be obtained once the image or screenshot of the memory of the palm device is obtained. There are two ways to obtain this logical data: either through HotSync or through physical acquisition of the RAM image file. Recall that physical acquisition method was explained in Section 8.4. The obtained information can then be used by the forensics examiners to trace the sources of attack.

8.4.3 Palm DD (PDD)

There was a mention of this tool in Section 8.3.2 (PDA Forensics). The PDD tool runs only on Windows-based systems and is mainly used by forensics examiners for physical acquisition. PDD does not have GUI support and everything has to be done from the command prompt of Windows. The tool also lacks support for bookmarking, search capability and report generation. A complete copy of the device's memory is acquired during the acquisition stage, and the data retrieved by PDD includes all user applications and

databases. Two files are generated from the information obtained. One file is a text file that has all the information pertaining to the palm device in investigation. The other file is created from the output sent by the user. Both these files contain an image copy of the palm device. The forensics examiner can then inspect these two files to find any evidence. There is an interoperability advantage because this tool also provides support for importing the files generated by PDD to EnCase tool for other forensics analysis on these files not supported by the PDD tool.

8.4.4 Forensics Card Reader

The Forensics Card Reader (FCR) consists of FCR software. It allows forensics examiners to acquire data from SIM cards without modification and a smart card reader with USB connection. The tool allows the examiner to select specific data elements that can be later stored and displayed in a finalized report. The reports consist of operations details such as case number, evidence number and examiner information. Such details can be automatically merged into the report. All data elements like phone directory, abbreviated dialling numbers, fixed dialling numbers, SMS messages, identifiers of the SIM and deleted SMS messages are acquired. The tool stores a complete report in an XML format. Extended phone book entries, including additional numbers and E-Mail addresses, can be acquired. The FCR reader allows examiners to use either small or large SIM cards without the need for an adapter. SIM cards for GSM mobiles as well as SIM cards for 3G mobiles can be used with FCR.

8.4.5 Cell Seizure

Cell Seizure is a forensics software toolkit. It is used for acquiring, searching, examining and reporting data associated with cell phones operating over CDMA, TDMA and GSM networks (see Box 8.1 to understand about CDMA, TDMA, GSM, etc.). By using Cell Seizure software, data can be acquired from cell phones, but a proper cable must be selected from either the Cell Seizure Toolbox or a compatible cable to establish a datalink between the phone and the forensics workstation. Cell Seizure has a number of features – bookmarking, automatic assembling of found images under a single facility and searching. Large type of data that can be obtained on most cell phones, using Cell Seizure includes:

1. **SMS history:** inbox/outbox.
2. **Phonebook:** SIM card, own numbers, speed dialling, fixed dialling.
3. **Call logs:** dialled numbers, received calls, missed calls.
4. **Calendar:** reminder, meeting, memo.
5. **Graphics:** wallpaper, picture camera images, EMS template images.
6. **Wireless Application Protocol (WAP):** WAP settings, WAP bookmarks.
7. **SIM:** GSM-specific data.

8.4.6 MOBILedit!

This is a forensics application that allows examiners to acquire logically, search, examine and report data from CDMA, Personal Communications Services (PCS) and GSM cell phones. The tool connects to cell phone devices through an Infrared (IR) port, a Bluetooth link or a cable interface. Once the connection is established, the phone model is identified by its manufacturer, model number, serial number and a corresponding picture of the phone. The data acquired from the cell phone is stored in a .med file format. After a successful acquisition, several fields get populated with data: subscriber information, device specifics, phonebook, SIM phonebook, missed calls, last numbers dialled, received calls, inbox, sent items, drafts and files folder. Items present in the files folder range from graphics files to camera photos and tones, and

depend on the phone's capabilities. Features of MOBILedit! include myPhoneSafe.com service that provides access to the IMEI database to register and check for stolen phones.

8.4.7 ForensicSIM

This toolkit comes from Radio Tactic. Its components include: acquisition terminal, analysis application, control card, data storage cards and the card reader. The toolkit deals with acquisition and analysis of data. Acquisition of data is carried out using the acquisition terminal which is a stand-alone unit that guides the examiner through each step of the acquisition process. Data analysis is carried out with the use of the ForensicSIM card reader, attached to a PC running the ForensicSIM analysis application. Forensics examiners use a control card to access the acquisition terminal and to prevent unauthorized use. The primary function of the acquisition terminal is to capture copies of the data from the target SIM to a set of data storage cards. ForensicSIM toolkit allows examiners read-only access to SIMs and generates textual reports based on the acquired content. Reports can be viewed internally, saved on disk or printed for presentation purposes.

Oxygen Forensic Suite 2010 is one more forensics product available in market for logical analysis of data found on cell phones, Smartphones and PDAs. Most commercial or free software are designed not only to view data but to upload data. This is not a safe way to perform a forensics examination. We live in a less than perfect world - some software marketed as forensics software warns that there can be a possibility of losing data. Device seizure does not allow data to be changed on the device. Paraben support is said to be available for unsupported cell phone models from supported manufacturers with simple log files and little time. Adding all this together, there is no comparison for forensics acquisition, analysis and reporting of hand-held device data.

8.5 Forensics of iPods and Digital Music Devices

In this section we focus on discussion about iPods and other hand-held devices available for music in digital form. Apple is the leading brand in the market today and there are three separate digital media players available from Apple Inc. All the players from Apple have the iPod brand – they are either the original iPod, the iPod Nano or an iPod shuffle. Irrespective of their type (i.e., original iPod, the iPod Nano or an iPod shuffle) all of these devices have the capability not only to play music but also to act as a storage device. It was mentioned in Chapter 3 (Section 3.7.4) that the lifestyle of today's young generation is such that they have embraced the mobile hand-held devices as a means for information access, remote working and entertainment! As this segment of tools, that is, iPods, is so important, in this section we discuss their forensics aspects. First, we understand the emerging modern nature of these devices, and then we explain iPod forensics techniques. There is a word of caution though – the discussion here is a conceptual contribution to the cyberforensics community. However, keep in mind that by no means this is a legal reference discussion. Therefore, we do not guarantee that the evidence, collected by following the guidelines of this section, will be admissible to a court. You should, as always, consult a lawyer/legal professional before attempting to collect evidence from an unknown situation.

8.5.1 The New Avatar of Digital Music Hand-Held Devices

Storage capacities of hand-held devices as well as the functionalities of PDAs are continuously improving. Many digital music devices have emerged with additional functionality than just playing music. Hand-held musical devices are taking on more PDA-like characteristics, such as the contact lists and calendar functions. These improvements have made the digital music device a technology that should be of interest to the cyberforensics community. Owing to the digital music revolution, digital music device has become a common household item. They are already making a natural progression into the criminal world.



Criminals can use the iPod with all its features in a variety of ways. Calendar entries may contain dates of crimes or other events that could be related to a crime. The contact information of conspirators or victims, along with photos or other documentation, could all be transferred and stored on the iPod.

Any of the files on the device may be of relevance to the case. One real-life example is the infamous use of an Apple iPod by a gang of thieves in England to store information related to their crimes.^[7] The iPod was used to store and pass information between the members of the gang about the cars they stole.

Modern digital music devices have large storage capacities as a result of improvement in storage technology. Some of the hard drive-based devices have capacities of 60 GB. With this large storage space for music, developers have added features like a calendar and contact book (e.g., the Apple iPods of various kinds – including the new naonochromatic series – see Fig. 8.21). These tiny devices are simply a portable hard drive and have the ability to store other types of files besides music, such as documents or pictures. An employee can walk away with sensitive information by using the capabilities of a digital music device and its USB interface.



Figure 8.21 | Apple iPods. (a) Apple iPod (regular), (b) Apple iPod mini, (c) Apple iPod (fourth generation) and (d) Apple iPod (nanochromatic series).
Sources: <http://www.letsgodigital.org>; <http://compstore.gmu.edu>; <http://regmedia.co.uk>; <http://www.bmw.com>

The employee could potentially store critical evidence on these types of devices. It must be determined if current frameworks of cyberforensics science are applicable and to what extent current guidelines can be applied to digital music device forensics. The other dimension of difficulty for digital forensics investigation comes from the large variety of these devices available to consumers and an abundance of proprietary OS and unique file structures.

8.5.2 Understanding iPod Features and iPod Forensics Techniques

As mentioned earlier, the iPod is the most popular digital music device. The iPod, though initially designed as a device to store and play music files, has evolved to become a mobile device that allows users to watch video, listen to music and store a wide variety of data. For example, drug dealers or loan sharks use an iPod like a PDA to store data in odd places and update their records right on the street without a PC. The newest versions of the iPod have become more PDA-like than ever before. Usually perceived as only a “music player,” people do not realize that all the extra functionalities possessed by the iPod can be more dangerous than portable hard drive because data can be read using its screen. This is a boon from forensics perspective though – because this feature of the iPod can provide clues in forensics investigation of a normal PC or lead to new evidence. However, an iPod may not always be included on a warrant for PC-related data. In general, iPods can be used for data storage with a lower likelihood of being identified or seized.



iPod can be more dangerous than portable hard drive because data can be read using its screen. As mentioned before, the iPod, with this new functionality has recently found its way into the criminal world.

With the continued growth of the digital music device market, iPod’s use in criminal activity is also continually increasing. With the iPod taking on more PDA and storage-like characteristics, investigators must understand how to deal with iPods; therefore, in the discussion here we are going to outline what should be considered when an iPod is found at the crime scene, and what it means in terms of critical analysis of some common forensics tools and their ability to collect and analyze data from an iPod. As mentioned before, iPod (see Fig. 8.21) is a digital device that can hold any type of file. These unique devices are, therefore, of interest to a forensics examiner. Apple has branched out and included additional applications. iPod now has a contact book, a calendar and other features. The newest version can even display photos on a color screen. These types of devices are already very popular and 10 million+ have already been sold. A first responder is currently not prepared for these types of devices and there is no documentation on how well the common tools, used by cyberforensics practitioners of today, work with the iPod. There are two versions of iPod: the Macintosh version that uses the HFS+ file system and the Windows version that uses the FAT file system. These versions each have unique requirements for the recovery of information from them.

Let us understand some of the key features of the iPod. In disk mode, the iPod can store other types of files, such as documents or pictures. With proper configuration, an iPod can run Linux and even contain all the necessary information for a computer system to run effectively. This helps users to carry their computer around with them and also allows them to boot it via their iPod attached to any computer. The iPod uses the Apple HFS+ file system when the device is run with an Apple system and the FAT32 file system when used with a Windows PC. The differences in these file systems make each version of the iPod a little different. Therefore, an individual who wishes to forensically analyze an iPod must be aware of the type of device with which he/she is dealing. The iPod can be configured with a variety of capacities. Although all iPods run similar software, there are four different generations and now there is also an iPod photo characterized

by some additional features. For storing contact information the iPod uses the standard vCard file format. Industry standard vCalendar format is used for storing calendar entries. Music is stored in a range of folders on the device and can be played in AAC, MP3 and other file formats. These are the main types of files and they constitute the majority of information stored on the iPod. However, users can store any file they wish on the device including encrypted or hidden files. Commercial accessories will allow an iPod to be used for a variety of functions including voice recording and digital camera photo storage. The legal considerations are explained in Box 8.6.

Box 8.6 iPod Forensics – Legal Considerations

When evidence is being prepared for possible submission to court proceedings, it is important for it to be collected in a "forensically sound" manner. Recall that definition of "forensically sound" evidence was provided in Chapter 7 (Section 7.15.1). Students of law course may like to visit the links provided at the end of this box to refer to the famous Merrell Dow Pharmaceuticals case that illustrated the "rules of scientific evidences." Well-documented and commonly accepted tools and techniques are necessary for admissibility under the Daubert criteria (see the note at the end of this box). Care must be taken to ensure that evidence collected from an iPod meets these criteria.

Owing to the iPod's large capacities and increased functionality, the cyberforensics and law enforcement community should treat it in a similar manner like they treat a suspect's hard drive. Suspects could potentially store key evidence on the iPod, and thus, a proper method for handling this type of evidence must be developed. This poses an interesting challenge for the forensics examiner, especially in terms of collection and analysis.

The following links (accessed on 19 April 2010) can be referred for the Merrell Dow Pharmaceuticals case of 1993. The *Daubert v. Merrell Dow Pharmaceuticals* lawsuit is a historical one. This case has had a lot of effect on similar cases and has changed the way the legal system looks at expert witnesses. The case is referred to here.

1. http://en.wikipedia.org/wiki/Daubert_v._Merrell_Dow_Pharmaceuticals
2. <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=509&invol=579>
3. <http://www.scumdoctor.com/Medical-Negligence/Daubert-V.-Merrell-Dow-Pharmaceuticals-Lawsuit.html>
4. <http://www.law.cornell.edu/supct/html/97-1709.ZS.html>

Below are some links (accessed on 18 April 2010) for The Kumho Tire Co. Ltd. v. Carmichael case of 1999. This case of Kumho Tire Co. Ltd. v. Carmichael extended these criteria to technological and engineering evidence.

1. http://en.wikipedia.org/wiki/Kumho_Tire_Co._v._Carmichael
2. <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=000&invol=97-1709>
3. <http://www.law.cornell.edu/supct/html/97-1709.ZS.html>
4. <http://www.computerlegalexperts.com/user/Kumho.pdf>

Note: "Expert witness" was mentioned in Section 7.7.1 (Chapter 7). In the same section "Daubert Hearing" hearing has also been mentioned.



When the iPod is taken to the laboratory for analysis, it is important to report the type of computer or computers that are found on the scene.

The name of the computer with which the iPod was initialized is stored on its drive. This information will be very useful in linking any evidence found on the device to the computers at the scene and then to the suspect. Finally, some settings were used for determining if an iPod is formatted for Macintosh or Windows. This was done on the device itself by selecting: “Settings >” then “About >”. When scrolling down in the “About” display, “Format: Windows” will show at the bottom of the screen if it is formatted for Windows. If that phrase is not found, it is normally assumed that it is an HFS+ formatted Macintosh iPod. With this background, we now consider iPod Forensics techniques. According to forensics experts, EnCase is the most suitable forensics tool for collection of forensics data from Mac as well as Windows version of iPod. The approach to forensics is outlined below:

1. Remove device from packaging
 - Photo and document everything
 - Charge device's battery
 - Start the device
 - (a) Select English and note any other settings
2. Mac version testing
 - Connect to Mac
 - Record information found on device
 - Connect to a Windows machine via firewire (without iTunes)
 - (a) Explore media via forensics tools.
 - Connect to Mac
 - (a) Explore use with Mac and iTunes
 - (b) Add contacts; add calendar
 - (c) Upload files (Microsoft Word, JPEG image and text file)
 - Use MFS tool via firewire
 - (a) Explore media
 - Connect to a Windows machine via firewire (without iTunes)
 - (a) Explore media via forensics tools
 - Connect to Mac and delete all information
 - Use MFS tool via firewire
 - (a) Explore media
 - (b) Attempt to recover deleted information
 - Connect to a Windows machine via firewire (without iTunes)
 - (a) Explore media via forensics tools
 - (b) Attempt to recover deleted information
3. Windows version testing
 - Connect to windows system
 - (a) Install iTunes and iPod Updater
 - (b) Reformat
 - (c) Documents changes to the device
 - (d) Explore features in Windows
 - Run forensics software (Mac and Windows) to recover old files on device before reformat
 - On Windows system
 - (a) Upload files (Microsoft Word, JPEG image and text file)
 - Use Windows forensics tools
 - (b) Find files

- Connect to Mac and use MFS
 - (a) Find files
- Delete files from Windows machine
- Use Windows forensics tools
 - (a) Recover deleted files
- Connect to Mac and use MFS
 - (a) Recover deleted files

Before moving onto the next section about crime scene considerations in the context of iPod forensics, a few important points must be mentioned here. The iPod keeps a persistent record of the computer with which it is initialized; the username of the computer user's and the computer's name are saved. This information is located just underneath the iPod device name in several locations on the drive. An analyst using a string search for the iPod's name can easily find these other two entries.



The username is directly underneath the iPod name and the computer name is underneath the username in the "DeviceInfo" file in the iTunes folder under the iPod_Control folder and in other places on the drive.

This information can be potentially useful in cases that hinge on connecting the device to a particular user, account or computer system. If the username stored on the iPod is the same as the username of the Mac computer that it was attached to, the iPod can be linked to the suspect's computer and to the suspect's account.



The calendar and contact entries are also easily found on the iPod by doing a string search.

The standard vCard and vCalendar formats store the entries on the hard drive in plain text and the information can be found by searching the hard drive for the strings in the header of the file. A calendar entry is stored with the file header of "BEGIN:VCALENDAR." The contacts can be found with the file header "BEGIN:VCARD." Beginning of each vCalendar or vCard entry is noted in these file headers and this metadata remain even after a file is deleted. The iPod also has another investigation friendly characteristic. It appears that the iPod stores information using the entire disk from beginning to end before returning to the beginning to store information again in areas that may have been deleted.

8.5.3 iPod Forensics: Evidence Handling and Crime Scene Considerations

As mentioned before, the iPod is one of the most popular digital music devices in today's marketplace. The newest versions of the iPod have become similar to PDA/storage like never before. With this new functionality the iPod has found its way into the criminal world.



The market for digital music device is continuously growing - with that comes higher use of iPods in criminal activity!

Therefore, it becomes necessary to search a physical crime scene and a suspect's personal belongings such as digital music devices. This is because many new digital devices have become common in the physical crime scene and the digital music device is one such device that will now be frequently found. Here are some important considerations when an iPod is found at a crime scene:

1. Before collecting any evidence, the first responder should wait for the advice of a forensics specialist.
2. Documentation of device location on the crime scene should be noted taking a photograph of its location along with the photograph of anything around the device.
3. The device should be left in its current state, as it is possible that the device could be booby trapped with a delete command set to execute if the device is disconnected from a charger or computer.

When collecting the device, its state at the crime scene should be noted. When you find that the device is connected to a computer at the scene, it is good to check and confirm if the device is mounted. Determining whether a device is mounted can be done by looking at the screen of the iPod – if it says “Do Not Disconnect” it is then necessary to unmount the device before disconnecting it from the computer. You can do this by dragging the icon of the iPod to the trash can on the Macintosh desktop. It is important to note the name of the iPod on the desktop before unmounting it. It is not a good idea to simply disconnect or unplug the computer, because the iPod’s disk could be damaged if not disconnected properly. If the iPod is connected to a Windows machine, it is recommended that it also be unmounted by clicking the “unplug or eject hardware” icon on the task bar on the bottom right of the screen. The type of machine the device is connected to will give the forensics analyst a better idea of what type of tools to use when analyzing the device. This information should be recorded and should be kept handy along with the documentation of the iPod.

When it comes to “preserving the digital evidence,” the iPod should be stored in the same manner as a hard drive – in a static free bag – and marked as “evidence.” Recall that “preservation of digital evidence” was explained in Chapter 7 (particular under the concept of “chain of custody” addressed in Section 7.8 and in Box 7.12). Antistatic bags for handling digital evidences are depicted in Fig. 8.22; the storage of evidence



Figure 8.22 | Antistatic bags for handling digital evidence.
Sources: <http://www.google.co.in>; <http://www.ojp.usdoj.gov/>; <http://www.alertsecurityproducts.com/>; <http://adventuresinsecurity.com/>; <https://www.ekitsupply.com>

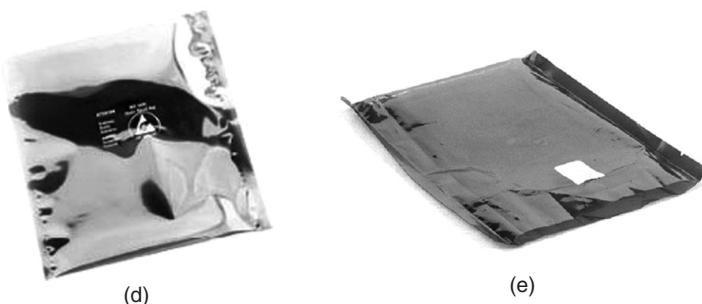


Figure 8.22 | (Continued)

is also depicted there; they are similar to the “Faraday Bags” depicted in Fig. 8.2 under Box 8.2. The iPod should not be stored near magnets or magnetic objects, which can cause magnetic interference and that could damage evidence on the iPod. Traditional good evidence procedures should be followed and the “chain of custody” should be thoroughly documented (chain of custody is explained in Section 7.8 in Chapter 7). Unlike some PDAs, the iPod need not be connected to a power supply while in storage. The contents of the device’s hard drive will not be lost if the device loses power. It is important to note, however, that it is possible for the battery to drain to a point where it may not be possible to charge it again and will need to be replaced. Although this is unlikely, it is possible in cases where an iPod may remain in storage for several years.

8.6 An Illustration on Real Life Use of Forensics

Having discussed forensics of small hand-held devices, here is an illustration showing how mobile phone forensics was used in a murder case mystery. Name of the victim has been masked for reasons of confidentiality and privacy. Sheila, a 17-year-old junior college girl had not returned home in a Bombay suburb till about 11:00 p.m. Having waited for a long time, hoping that Sheila would eventually return, her mother finally gave up. She was very worried as returning so late was not known to be Sheila’s habit. At around 1:00 p.m., Sheila’s mother called up local police station to make a complaint about her missing daughter. Sheila’s mother was aware that Sheila had gone out that day with her friends. The friends told her mother that they had accompanied Sheila till about 1 km away from her house and from there on they had parted their ways. Sheila’s mother also told police that she had made several calls on Sheila’s mobile phone and the last time the phone had rung was about 10:30 p.m. after which there was no response. Her mother thought that perhaps the phone was switched off after that time and she was very worried not having heard from her daughter. After making a few enquires, the police came to know that Sheila was last seen walking toward her residence with her friends that day at around 7.30 p.m.

The police then decided to hand over the case to special crime investigation cell. The mobile service provider was contacted to find out the location of Sheila’s mobile phone at the time when it rang the last time. Till the time a mobile phone is switched on, its location can be determined by the mobile service provider to the precise point or within a margin of about 2 meters. At the worst, the margin of error could be about 5 meters. The time taken for a pulse from the transmission tower, to the activated mobile handset along with the angle to show its direction, can be used to precisely determine the point of its location. This way, a person carrying a mobile phone can be tracked. In this case, the mobile service provider could locate but could not physically find Sheila’s mobile handset. It was located to be about 500 meters away

from the place where her friends had parted their ways after being last seen with Sheila. Initial investigations with her friends did not yield any clues. However, when the computer in Sheila's room was examined, it turned out that Sheila had been frequently chatting on the Internet with person/identity named "junkymoney."

Now a technical team was invited into the investigation. They found that Sheila's last chat with "Junkymonkey" was at about 12:00 noon on the day she was reported missing. The regional IP address was requisitioned for the details of the identity "junkymonkey." The technical team examined the traces of Sheila's regular chat with the identity "junkymonkey." Using the IP address, investigators zeroed onto two houses. However, *prima facie*, nothing obvious and related to the case was observed. In one of the zeroed houses, there was an elderly couple and so that house was ruled out from the investigation. In the other house lived a middle aged couple with their son Sunny, about 20 years old. On further enquiry, it was found that Sunny's parents were away on that day when Sheila had disappeared. When investigators seized Sunny's computer system and examined it; it revealed username "junkymonkey." They scrutinized the contents and timing of search history of Sunny's computer. Cookies on the computer revealed that there were repeated searches made that day on strings such as "Why dead bodies float in Water," "How to block dead bodies from floating in Water," "Deepest point in ... (lake)" etc. IP address details of the account created with the name "junkymonkey" linked to "suspect machine" in the house searched. Further investigations with Sheila's chat traces confirmed that the id, with which Sheila had been chatting, matched with the account id found on Sunny's machine.

Sunny was arrested and taken in for interrogation. He broke down confessing to the disposal of Sheila's body in the lake nearby. The body was found punctured with several wounds in the stomach and chest, in addition to an injury in the head. Sunny further confessed that he was in love with Sheila but she would never respond to his overtures. Further confession from Sunny revealed that the day on which Sheila was reported missing, Sunny had called Sheila over to his house. Sunny had tried exploiting the situation of being alone in his house with Sheila that day while his parents were away. To save herself from Sunny, Sheila fiercely resisted his attempts of intimate contacts with her. In the course of physical fight with Sunny, Sheila had stumbled upon very sharp object in the house and sustained a fatal injury into the head leading to her death. Sunny was very scared as he could not have kept the dead body in the house knowing his parents were to return the next day. For clandestine disposal of Sheila's body in the nearby lake, he surfed the Internet for answers to his queries about sinking a dead body!

8.7 Techno-Legal Challenges with Evidence from Hand-Held Devices

Hackers are getting sophisticated (recall Figs. 7.21 and 7.22). This is true for mobile phone-based crimes as well as crimes performed with other small hand-held devices. When starting from digital data acquired from a desktop drive, mobile phone memory or network trace, forensics examiners must ensure the integrity of the entire investigation; this includes evidential integrity too.



"Forensically sound" evidence is required for presentation in the court.

Table 8.7 | E-Discovery and computer forensics: The difference

<i>E-Discovery</i>	<i>Computer Forensics</i>
<ul style="list-style-type: none"> • E-Discovery means “gathering,” “searching,” “filtering” and producing large amount of information for the purpose of review • Data is accessed by not analyzing • Active as well as archived data is involved • Normally does not include deleted data, does not include discarded or hidden data • Back up tapes, E-Mail servers and network servers are in scope • May or may not include metadata 	<ul style="list-style-type: none"> • Computer forensics involves investigation and detailed analysis • Typically targeted at selected hard drives of PCs where the evidence is believed to exist • May include backup tapes • Data analysis is a key phase • Will typically involve searching for “deleted” files • Re-creation of time critical events is done • Determining “who,” “what” and “when” • Breaking passwords/encryption is involved • Reporting and expert testimony is involved • Metadata (data about data) plays a key role

Note: See Box 7.3 in Chapter 7.

At the start, the authenticity and integrity of an acquired disk or memory image can be managed, along with information about data provenance and chain of custody, using one of several file formats. Although this may well be, there seems to be a considerable gap between law enforcement and organized crime when it comes to the utilization of mobile phone technologies. Mobile phones and pagers were used in the early 1980s by criminal organizations as a tool to evade capture as well as a means to facilitate everyday operations. Ironically, while it took decades to convince legitimate businesses that mobile connectivity can improve their operations, just about every person involved at any level of crime already knew in the early 1980s that mobile phones can provide a substantial return on investment! The difference between computer forensics and E-Discovery is explained in Table 8.7. This is important because many people do have confusion between the two. In the next section we provide an overview of how computer forensics is used in litigation and then end with specifics on hand-held device-related “evidences” with guidelines and challenges (Sections 8.7.6 and 8.7.7).

8.7.1 Role of Computer Forensics in Litigations

Computers have appeared in the course of litigation for several years.



The arrival of computers in commercial disputes and in criminal cases did not create immediate difficulties as judges sought to allow computer-based evidence on the basis that it was not any different from traditional forms of evidence.

The ultimate aim of a forensics investigation is that the evidence can be used in legal proceedings. As we have learned by now, forensic computer examinations are unlike ordinary data recovery efforts. Forensics computer examinations use strict controls and procedures to ensure that all existing data is found, that the original data is preserved unchanged and that any recovered data is admissible in court or other legal proceedings. Deleted, disguised, hidden and password-protected data can be retrieved in many instances. The forensics examiner is able to recover many forms of data which are not readily accessible. The recovered data would then be carefully documented, catalogued, analyzed and recorded in exhibits, and reports would

be presented to the client or the courts in compliance with the rules of evidence. There is an interesting quote by Judge James M. Rosenbaum:

"Computer's DELETE key acts somewhat like a thief who steals a card from the old library's card file. When the card was in place, the librarian could decode the library's filing system and find the book. If the card was gone, or unreadable, the book was still in the library, but it could no longer be found amidst the library's stacked shelves. In a computer, the 'lost' book can be found with very little effort!"

When it comes to court procedures, knowing legally accepted procedures is important. Recall the principle of "forensically sound" evidence explained in Chapter 7 (Section 7.15.1). The most common legal difficulty is having digitally based evidence accepted in court. Data collected for the purposes of evidence must be shown to be untampered with and fully accounted for, from the time of collection to the time of presentation in the court. Therefore, it must meet the relevant evidence laws. As such, computer forensics experts must have a good understanding of the legal requirements as well such as evidence handling, storage and documentation procedures. An impartial computer expert may get called as "expert witness." Such expert who helps during discovery will typically have experience on a wide range of computer hardware and software. This is beneficial when the case involves hardware and software with which this expert is directly familiar. However, fundamental computer design and software implementation is often quite similar from one system to another, and experience in one application or OS area is often easily transferable to a new system. The situation is different as compared to "paper evidences." Unlike paper evidence, computer evidence can often exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of their existence, even alternate formats of the same data can be discovered. The discovery process can be served well by a knowledgeable expert identifying more possibilities than can be requested as possibly relevant evidence. In addition, during onsite premises inspections, for cases where computer disks are not actually seized or forensically copied, the forensics expert can more quickly identify places to look, signs to look for and additional information sources for relevant evidence. These may take the form of earlier versions of data files (e.g., memos and spreadsheets) that still exist on the computer's disk or on backup media, or differently formatted versions of data, either created or treated by other application programs (e.g., word processing, spreadsheet, E-Mail, timeline, scheduling or graphic).



From "integrity" perspective, protection of evidence is critical (recall the "chain of custody" concept explained in Chapter 7).

A knowledgeable computer forensics professional will ensure that a subject of computer system is carefully handled to ensure that the following:

1. Potential evidence is not damaged, destroyed or otherwise compromised by the procedures used to investigate the computer.
2. There is no possible computer virus threat introduced to a subject computer during the analysis process.
3. The investigation team is properly handling and protecting the extracted and possibly relevant evidence so that it is not impacted from later mechanical or electromagnetic damage.
4. Continuity of chain of custody is established and maintained.
5. Business operations are not majorly impacted.
6. Any information pertaining to client–attorney is ethically and legally respected and not divulged – such information could have been inadvertently acquired during a forensics exploration.

The main advantage of a computer forensics examination comes from an ability to search through a mountain of data very thoroughly and quickly and in any language. This enables legal professionals to produce as evidence data which would otherwise not be produced to the court. The ability to recover data which has been deleted, damaged, hidden or lost is of great advantage to legal professionals involved in litigation.

Computer evidence in the court is used by the following entities:

1. **Criminal Prosecutors:** They use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record keeping and child pornography.
2. **Civil litigations:** They can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination and harassment cases.
3. **Insurance Companies** may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson and workman's compensation cases.
4. **Corporations** often hire computer forensics specialists to ascertain evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.
5. **Law Enforcement Officials** frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
6. **Individuals** sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment or age discrimination.

Box 8.7 SMART Forensics Tools

SMART stands for Storage Media Archival Recovery Toolkit. It is used with Linux OS. It is developed by ASR Data Acquisition and Analysis LLC. This software utility has been designed and optimized to support data forensics practitioners and information security personnel in pursuit of their respective duties and goals. The SMART software and methodology was developed with the intention of integrating technical, legal and end-user requirements into a complete package that enables the users to perform their job most effectively and efficiently. SMART is more than a stand-alone data forensics program. The features of SMART allow it to be used in many scenarios, such as:

1. "Knock-and-talk" inquiries and investigations;
2. onsite or remote preview of a target system;
3. postmortem analysis of a dead system;
4. testing and verification of other forensics programs;
5. conversion of proprietary "evidence file" formats;
6. base lining of a system.

SMART is basically a data forensics program that runs on both BeOS and Linux OS. SMART is sold and marketed as a feature-rich data forensics utility with functionalities such as media hashing, media imaging, media restoring and media wiping. SMART is currently utilized by Federal, State and Local Law Enforcement, US Military and Intelligence Organizations, accounting firms, data forensics examiners, data recovery specialists, disaster recovery professionals, information security professionals, healthcare privacy professionals' internal auditors and system administrators. Both Law Enforcement and Corporate communities have accepted SMART. Another tool that is quite popular is "Maresware." It was developed by Mares and Associates for investigating computer records while running under the LINUX OS on Intel processors. It is useful to all types of investigators, including law enforcement, intelligence agency, private investigator and corporate internal investigator. When used within a forensics context, the software enables discovery of evidence for use in criminal or civil legal proceedings. Internal investigators can develop norms and document those norms to support disciplinary actions; yet they do so non-invasively to preserve evidence that could end up in court.

It must be borne in mind, however, that in a case where computer forensics examinations have been conducted, the legal practitioners involved must have extensive knowledge in computer. Without a comprehensive knowledge of computers, it would be extremely difficult to cross-examine a computer forensics expert. Similarly, it is possible that providing an appropriate ruling would be difficult without a thorough understanding of how computer systems work.

8.7.2 Challenges Due to Forensics Validity Issues about Evidences

There are many issues and challenges. Such issues can pose a threat to the validity of mobile phone forensics. For example, there are difficulties in acquiring certain types of data that stem from the proprietary nature of mobile phones. In addition, features such as Bluetooth and the ability to run third-party applications can create additional problems. As a result, mobile forensics tools are struggling to reliably acquire data from a wide range of mobile phones. As the amount of evidence and different types of mobile phones increases, the tools and technology must also catch up to include features and functionalities to accommodate these changes without sacrifice. As another example, consider Oxygen's Mobile Phone Manager, the phone synchronization tool used for at least 2 years by law enforcement to gather evidence from mobile phones before being updated. April 2007 saw the release of an updated tamper-resistant "forensics" version – this version is said to use hash values to help maintain the integrity of acquired data. Before this version was available, it was unclear how integrity management was addressed. As we learned in Chapter 7, when it comes to the admissibility of such evidence in court, the evidence has to be "forensically sound." Mobile forensics tools have not got the capability to address the issue of evidence integrity management. Proprietary OS on mobile phones is still an issue that has implications in data integrity.



Proprietary OS makes retrieving information from phone memory difficult.

Some of the current mobile forensics tools claim that they acquire evidence from mobile phones in a forensically sound manner, and maintain their integrity upon further examination. The aim behind "forensically sound evidence" is to make it admissible in the court of law. Achieving this aim is possible only if the integrity of the evidence remains intact (recall the concept of "chain of custody" explained in Section 7.8 in Chapter 7 and the related concepts in Figs. 7.10 and 7.11, Boxes 7.4 and 7.12). The methods used to acquire and manage evidence are best if understood and accepted by a majority of mobile forensics professionals. There are many unknowns and assumptions in mobile forensics practice.

8.7.3 Challenges to Law Enforcement Authorities

There are additional challenges apart from the "evidence integrity" issues mentioned in the previous section. When it comes to dealing with digital evidence obtained from mobile devices, law enforcement and digital forensics still lag behind. This could be partly due to some of the following reasons:

1. Specialized interfaces, storage media and hardware are required to support evidence extraction given the mobility aspects of modern hand-held devices;
2. the difference between file system residing in volatile memory vs. stand-alone hard disk drives;

3. hibernation behavior in which processes are suspended when the device is powered OFF or is idle but at the same time, remaining active;
4. the diverse variety of embedded OS in use today;
5. the short product cycles for new devices and their respective OS.

Due to these differences, it becomes important to distinguish between mobile phone forensics and computer forensics. Let us understand this.



A key difference between computers and mobile phones is the data storage medium. While volatile memory is used to store user data in mobile phones, computers use non-volatile hard disk drives instead as a storage medium.

For mobile phones, this implies that if the mobile phone is disconnected from a power source and the internal battery is depleted, user data can be lost. On the contrary, with non-volatile drives, even when the source of power is disconnected, user data is still saved on the hard disk surface and there is no risk of deletion (even when the power source is OFF). From a forensics perspective, evidence on the mobile phone device can be lost if power is not maintained on it. In that case, investigators must ensure that the mobile device has a power supply attached to it so that data on the device is maintained (forensically sound digital evidence). One of the drawbacks that mobile OS and mobile phone forensics development currently face is the extremely short OS release cycles. Symbian, a well-known developer of mobile phone OS, is a prime example of the short life-cycle of each of its OS releases. Symbian produces a major release every 12 months or less with minor releases coming in between those major releases. This short release cycle supports timely development, testing and release of forensics tools and all the updates that deal with the newer OS releases difficult to achieve.

There are challenges from the hardware side as well, when it comes to mobile phone forensics. Mobile phones are portable devices designed and meant for a specific function unlike computers that are made for a more general application.



Mobile phone hardware architecture is designed keeping in mind features such as mobility, extended battery life, simple functionality and light weight. Owing to this architecture, the general characteristics of a mobile phone are very different from those of a computer in the way it uses the OS, how its processor behaves and how it handles its internal and external memory.

The hardware architecture of a typical mobile phone usually consists of a microprocessor, main board, ROM, RAM, a radio module or antenna, a digital signal processor, a display unit, a microphone and speaker, an input interface device (i.e., keypad, keyboard or touchscreen) and a battery. The OS usually resides in ROM whereas RAM is generally used to store other data such as user data and general user modifiable settings. The ROM may be reflashed and updated by the phone user by downloading a file from a website and executing it on a PC that is connected to the phone device.

8.7.4 Toolkit Constraints

There are constraints for forensics tools and toolkits too and that is for historical reasons. When initially mobile phones came into market, they did not have the capacity for large amount of information storage. In those days, therefore, law enforcement officers had no need to access mobile phone handsets to get

information on a suspect. The focus was more on phone records from the telecommunications companies. Modern day mobile phones have very large storage capacity as well as a wide range of applications running on them. Today's mobile phones also have additional connectivity options in addition to the connectivity with the telecommunications provider. Mobile phone forensics tools and toolkits, however, are still considered to be immature in dealing with these advances in mobile phone technology.



There are third-party companies that develop mobile forensics toolkits. However, the toolkits are not independently verified or tested for forensics soundness.

The developers of the toolkits admit that they use both manufacturer-supplied and self-developed commands as well as access methods to gain data access to memory on mobile devices. Often, the tools may work with only a few phone manufacturer handsets and only a limited number of devices are supported. Some of the tools also have a limitation when it comes to connectivity options and also when it comes to acquisition of data from the handset. For example, some tools are limited to wired connections as opposed to Infrared (IrDA) and Bluetooth access to data on mobile devices. There is one more problem - while some toolkits do have acquisition capabilities, they do not have the features for evidence examination or reporting facilities. Moreover, direct access to data on the mobile phone is not achievable. Phone software and/or hardware needs to be used for acquiring data from the mobile phone's memory. This innate difference between computer forensics and mobile phone forensics has an impact on how data acquired from mobile phones is perceived.

Evidences get probed into and there are "rules of evidence." In legal terms, "probative value" means an evidence that is sufficiently useful to prove something important in a trial. For this, the probative value of proposed evidence must be examined against prejudice in the minds of jurors toward the opposing party or criminal defendant (for more on "probative evidence" refer to Ref. # 22, Additional Useful Web References, Further Reading. Link to a good paper on this topic is provided under Item # 18 under Articles and Research Papers and Technical Documents). Digital Evidence is "*information of probative value which is stored or transmitted in binary form.*" As per this definition, evidence is not just limited to what is found on computers but may also extend to include evidence found on digital devices such as telecommunication or electronic multimedia devices.

Digital evidence is different from the "traditional" evidence – it is not only limited to traditional computer crimes such as hacking and intrusion, but it is more extensible and includes every crime category in which digital evidence can be found. "IT Evidence" is a tricky term not only because its definition is difficult but also because it can vary from legislation to legislation. For example, if IT Evidence is considered as: "*any information, whether subject to human intervention or otherwise, that has been extracted from a computer. IT evidence must be in a human readable form or able to be interpreted by persons who are skilled in the representation of such information with the assistance of a computer program*"; then there is a problem with this definition because it does not address evidence on digital devices other than a computer. This implies that digital evidence definitions or procedures related to digital devices may not always get updated to address mobile phone evidence.

8.7.5 Generally Accepted Evidence Principles and the Difference with Hand-Held Devices

Principles that are generally accepted in the forensics community about computer-based electronic evidence are as follows:

1. Actions taken by law enforcement agencies or by their agents should NOT modify *data held on a computer or storage media* because this is the data on which in the court relies upon.

2. Exceptional circumstances are to be considered - for example, there may be a situation wherein it becomes necessary for an individual *to access original data held on a computer or on storage media*. In such a case, *that person must be competent to do so* and should be able to present evidence to explain the relevance and the implications of actions taken.
3. An audit trail or other record of processes applied to computer-based electronic evidence should be created and preserved (recall chain of custody concept explained in Section 7.8, Chapter 7). Those processes should get examined by an independent third party to confirm that the same result is achieved.
4. The person responsible for the overall investigation must ensure that the law and these principles are adhered to.

These principles are only recommended best practices or generally accepted good principles and not following these above guidelines may not necessarily mean that the evidence collected is not considered as viable evidence. There are some more points to ponder with regard to the above-mentioned principles because they are important:

1. When it comes to *mobile phone forensics*, Principle 1 mentioned above, compliance may be difficult. This is because the nature of mobile phone storage and the underlying technology is continually changing and “change to data held on the device” may happen automatically without interference from the mobile user. Thus, the goal of *mobile phone data acquisition* should be “to affect the contents of the storage of the mobile as less as possible” and adhere to the Principle 2 and Principle 3 (mentioned above) to focus more on the competence of the specialist and the generation of a detailed audit trail.
2. In adhering with Principle 2, the *specialist must be competent* enough to understand the internals of both hardware and software of the specific mobile device they are dealing with as well as have an expert knowledge of the tools they are using to acquire evidence from the device.
3. More than one forensics tool may be used when acquiring evidence from mobile phone. This is because some tools do not return error messages when they fail in a particular task. At times, this can be a debatable issue if “evaluation,” “calibration” and “standardization” aspects of forensics tools were to be considered.^[8]
4. When it comes to adhering with Principle 3, providing a thorough record of all processes used to obtain the evidence in a way that can be duplicated by an independent third party is essential in order for the evidence gathered to be admissible in court.

Given the dynamic nature of Smartphones, the principle of NOT taking actions that could change the evidence cannot be applied to evidence recovered from Smartphones.

Furthermore, mobile phone acquisition tools that claim to be forensically sound do not directly access the phone’s memory but rather use commands provided by the phone’s software and/or hardware interfaces for memory access and thus rely on the forensic soundness of such software or hardware access methods. Therefore, when using such tools, the ability to extract information in a manner that will not significantly change the mobile phone’s memory is not verifiable.

8.7.6 Mobile Phone Evidence Guidelines

As part of mobile phone evidence guidelines, remember the following:

1. If the device is “ON,” do NOT turn it “OFF”.
2. Turning it “OFF” could activate lockout feature.
3. Note down all the information seen on the display (photograph if possible).

4. Shut down the power before transporting the evidence (take any power supply cords present).
5. If the device is “OFF,” leave it “OFF.”
 - Turning it ON may result in altering evidence on device (same as for care to be taken for evidence residing on computers).
 - Upon evidence seizure, take it to an expert at the earliest possible or get in touch with local service provider.
 - If an expert is unavailable, *use a different telephone* and contact the expert.
 - Make every effort to refer to relevant instruction manuals pertaining to the device.



Typically, potential evidences considered from small hand-held devices are appointment calendars/information, password, caller identification information, phone book, electronic serial number, text messages, E-Mail, voice mail, memos and web browsers. However, it should not be forgotten that mobile devices could have external storage attached to them.

A mind that has a constant suspicion is a good mind for a forensics investigator! Even, other equipments such as fax machines may contain such external storage devices. Other electronic items - cellular phone cables, cloning equipment, etc. – should also be considered since they may contain information of evidentiary value.

Mobile phones may have several items residing on them – for example, electronic documents, handwriting information, location information, etc. Evidential significances are associated with phone-based applications such as Symbian, Mobile Linux and Windows Mobile. Both Windows and Symbian Mobile-based phones are known to execute Malicious Code, such as Trojans and viruses (together known as “malware”), especially those malwares that were transferred via Bluetooth technology. Non-malicious applications on mobile phones also need to be considered as evidence because they may get used for conducting illegal activities. Moreover, they (i.e., non-malicious applicatons on mobile phone) may store log files or any other form of data that could be considered as evidence. Thus, we can see that almost all phone applications and data related to them can be considered as potential evidence. This includes logs relating Bluetooth, Infrared (IrDA), WiMax and Wi-Fi communications and Internet-related data such as instant messaging data and browser history data. Many mobile phone OS support a version of Java; therefore, Java applications should also be considered as evidence.

When it comes to handling instructions for mobile phones, the following key principles should be remembered:

1. Evidence may get lost during any interaction with the handset on a mobile phone; therefore, it is important not to interrogate the handset or SIM.
2. Before handling the evidence, consider if any other evidence is required from the phone. In case additional evidence, apart from electronic data, is required, adhere to the general evidence handling procedures for that particular type of evidence laid out in the scenes of crime handbook. Alternatively, contact the responsible crime investigation officer in your area.
3. As mentioned before, general advice is to switch the handset OFF due to the potential for loss of data if the battery fails or new network traffic overwrites call logs or recoverable deleted areas (e.g., SMS); there is also potential for sabotage. However, investigating officers may require the phone to remain ON for monitoring purposes while live enquiries continue. In such a case, ensure the unit is kept charged and not tampered with. In all events, power down the unit prior to transport.

8.7.7 Battery and Memory Storage Considerations from Forensics Perspective



Typically, three types of batteries are used in mobile phones: Liion (lithiumion), NiMH (nickel metal hydride) and Lipolymer.

Lithiumion battery technology is also available - it allows recharging of batteries 60 times faster than conventional batteries. This means that it will take about a minute for a battery to go from being drained to being 80% charged. Over a period of time, fuel cell batteries have emerged as another type battery choice. However, these type of batteries are not yet available in mass production. Wireless communications, that is, the use of WiMax, Bluetooth and Wi-Fi, tend to drain batteries much faster even when used for simple computing tasks. This will present more challenges as these communication and connectivity options are becoming more natively integrated into today's Smartphones. Battery life can have a huge impact on a mobile forensics investigation as volatile data can be lost if the battery is drained.

The OS of mobile phones and the applications running on them are smaller in size compared to computer-based OS and applications. Therefore, it makes sense to store them in RAM, ROM or flash memory. Current high-end mobile phones may have 64–128 MB of static RAM for application code, 128–256 MB of flash memory for system code and more than 128 MB of flash memory for user data. The amount of RAM, ROM or flash memory is on the rise which means that data access and transfer rates to support them will improve. Technological advances and sophistication of electronic circuitry in external memory has made support go mainstream in higher end mobile phones. The physical sizes of such devices are becoming smaller and at the same time their storage capacities are increasing. On the down side, these devices have become very fragile and easily concealable by evil doers due to reduction in their size. What is more, some mobile phones allow the swapping of external storage memory in and out without having to turn OFF the mobile device or the need to even take out the battery cover. Auditing such devices on the mobile OS level must be addressed for mobile forensics reasons.

8.8 Organizational Guidelines on Cell Phone Forensics

A few words on the policy side are important to remember as a take away from this important section; on the cell phone forensics side, the guidelines are provided in Table 8.8.

8.8.1 Hand-Held Forensics as the Specialty Domain in Crime Context



Technology is advancing rapidly and when it comes to hand-held devices it is even growing quicker especially in their capabilities and in their use. With the continuous advancement in technology, it is not a surprise to come across those devices (either PDAs or Smartphones) which can contain as much processing power as would have held a normal desktop couple of years ago.

Table 8.8 | Cell phone forensics – Organizational guidelines

<i>The Guideline</i>	<i>Key Aspects of the Guidelines</i>
Organizations should make sure that their policies have clear statements about forensics considerations for cell phones	<ul style="list-style-type: none"> High-level policy should support authorized and competent forensics staff to carry out investigations of company provided cell phones when such investigation is required for legitimate reasons and under the appropriate circumstances. In the forensics policy, there should be clear definition of the roles and responsibilities of the workforce as well that of any external organizations – for performing or assisting with the organization's forensics activities. The policy should also mention internal teams and external organizations to be contacted under various circumstances.
Organizations should document and maintain procedures and guidelines to support forensics on cell phones	<ul style="list-style-type: none"> Guidelines should be based on general methodologies for investigation of incidents based on forensics techniques. Development of step-by-step procedures should be considered for carrying out all routine activities in the preservation, acquisition, examination and analysis, and reporting of digital evidence found on cell phones and associated media. The guidelines and procedures should facilitate consistent, effective, accurate and repeatable actions carried out in a forensically sound manner, suitable for legal prosecution or disciplinary actions. The guidelines and procedures should consider the admissibility of evidence in case of legal proceedings - this should include seizing and handling evidence properly, maintaining the chain of custody, appropriate storage of evidence, establishing and maintaining the integrity of forensics tools and equipment, and demonstrating the integrity of any electronic logs, records and case files. The guidelines and procedures should be reviewed periodically, and also whenever significant changes in cell phone technology appear that affect them.
Organizations should see to it that their policies and procedures support the reasonable and appropriate use of forensics tools for cell phones	<ul style="list-style-type: none"> Policies and procedures should clearly explain what actions are to be taken by a forensics unit under various circumstances commonly encountered with cell phones. They should also describe the quality measures to apply in verifying the proper functioning of any forensics tools used in examining cell phones and associated media. Procedures for handling sensitive information that might be recorded by forensics tools should also be addressed. Legal counsel should carefully review all forensics policy and high-level procedures for compliance with international, federal, state and local laws and regulations, as appropriate.
Organizations should ensure that their forensics professionals are competent enough to conduct forensics activities on cell phone	<ul style="list-style-type: none"> Forensics professionals, especially first responders to incidents, should be well aware of their roles and responsibilities for cell phone forensics and receive training and education on related forensics tools, policies, guidelines and procedures. Forensics professionals should also work closely with legal counsel both in general preparation for forensics activities, such as determining which actions should and should not be taken under various circumstances. In addition, management should own the responsibility toward supporting forensics. Capabilities, reviewing and approving forensics policy, and examining and endorsing unusual forensics actions that may be needed in a particular situation.

With those amazing hand-held devices, their storage capacities are phenomenal and keep increasing even though these digital devices are getting ultralight in weight.

Hand-held digital forensics has proven to be very versatile and useful, especially, if you are trying to look for hints of foul play. In the modern era, millions of people are relying on mobile gadgets wherein they store data, communicate and find some leisure. As these mobile tools hold a lot of information, they are also one way of proving dishonest activity in relationships and in the workplace.



The beauty of hand-held digital forensics is that it allows data to be retrieved even if the gadget or technology itself has been destroyed.

For example, the memory card or SIM card inside cellular phones is meant to store all incoming and outgoing information. With the help of advanced tools and forensics experts these cards can be accessed to find out all contained information. Most people who want to check and investigate simply need to bring the gadgets to a professional. They may also install other surveillance devices or programs into the material; however there may be the risk of them being detected by antivirus and other protection software and applications.

Digital forensics domain, for a long time, has focussed on traditional media such as hard drives. Even today, hard drives are the most prevailing common digital storage devices around. Therefore we can appreciate how these devices have become a primary point of evidence. As more and varied digital storage become available due to technological advances, forensics examiners need to gear up for the new possibilities of those modern devices holding digital fingerprints.



Cell phones and PDA devices are so common that they have become standard in today's digital examinations. Hand-held devices store personal information, voice calls and contact information that provides digital evidence during an investigation.

Forensics examiners have to follow clear, well-defined methodologies and procedures for proper retrieval and speedy examination of information present on the device. Cell phones are designed for mobility, they are compact in size, battery powered and lightweight; they often use registered OS, a Subscriber Identity Module (SIM) and a removal media. Cell phones operate on platforms like RIM, Pocket PC and Palm OS devices. SIM uniquely identifies the subscriber, determines the phone number and contains the algorithms needed to authenticate a subscriber to a network. A user can remove the SIM from one phone, insert it into another compatible phone and resume use without the need to involve the network operator.



The hierarchically organized file system of a SIM is used to store names and phone numbers, sent and received text messages, and network configuration information.

Cell phones are becoming so advanced that by using them it is possible to perform various functions such as browsing, E-Mail communication and storing files. Hand-held devices are rooted in their own OS, file systems, file formats and methods of communication. Dealing with these devices creates unique problems for examiners.



Performing a forensics exam on a cell phone or PDA is a sophisticated job; it requires special software and specialized knowledge about the way these devices work as well as where possible evidence could be stored.

The market for digital hand-held portable devices has shown a considerable growth. The market includes personal use digital music devices/MP3 players, Smartphones as well as common PDAs. With the growing technology, these PDAs have widely evolved and nowadays are equipped with in-built memory with a minimum capacity of 128 MB and some even more. Apple Computer has announced its digital music player with a capacity higher than 40 GB. Among all these digital devices, the PDAs have been designed to overcome the physical constraints set by either PCs or even laptops. Some of the major features of PDAs as compared to PC or laptops are listed below:

1. They are compact and ultralight, thus allowing mobility to the users;
2. They store user data on volatile memory, such as the RAM and ROM for the OS.
3. They also hang up processor when powered off to save rebooting time.
4. They provide organizing functionality such as E-Mails, calendars and memos.
5. They also offer the ability to synchronize data with a PC.

Given the architecture of PDAs, it is very difficult and very challenging to conduct sound forensics of these digital devices (i.e., PDAs) without specialized forensics toolkits, and without the proper procedures. In the PDA family, there are at present three main OS which share the market – Palm OS, Microsoft Pocket PC and finally portable Linux-based OS. These digital devices support some basic functionalities such as contact, E-Mail, task management and calendar known as PIM applications. As we are in the new age of technology evolution, the PDAs market share seems to have only two dominant players now – Palm OS and Microsoft Pocket PC. Another important feature of the latest Palm is that it has the ability to communicate through wireless medium, surf on the Web and even provide editing facilities for electronic document.

Although these PDAs allow a high level of mobility to their users, they also add up another special aspect to their reputation when it comes to storage of data on the PDAs, by introducing the use of removable media such as external media cards with enormous capacities ranging from 128 MB to 4 GB, thus, making the PDAs more attractive to the users as well as to the criminals.

It is necessary nowadays that the analysis of these hand-held devices be combined with the existing digital forensics procedures and methodologies already in place to keep up with the technology. Most PDAs available in the market are based on similar basic designs; however, they differ in their OS. Their hardware components, unfortunately do not facilitate the acquisition of forensics data on the hand-held devices without modifying their actual or current state. Even though this process is not quite easy to perform, the data acquisition can nevertheless be performed on the PDAs through some of the currently existing forensics software for that type of acquisition.

There is an increase in the use of powerful digital hand-held devices. The methodologies and procedures for the analysis of digital forensics are being re-examined, re-considered and re-executed with the objective to adapt to the new age of digital hand-held devices such as PDAs, portable digital music devices and mobile phones. While reconsidering the methodological approach to these new hand-held devices, there are two most crucial parts in sound forensic examining these devices, namely

1. Acquisition stage.
2. Authentication stage.

In the case of Palms, this task becomes even more delicate and important because, a great deal of accuracy is required. A crucial aspect of the PDA, with regard to the acquisition and analysis, lies in the use of their memory (i.e., both the RAM and the ROM). There are challenges when it comes to the storage of data on the PDA and the OS of the PDA. As RAM storage is volatile, the PDA is powered by a battery that allows the memory to be kept alive for storing of data on the PDA.

Carrying forensics analysis or acquisition on PDA device would be very risky as operation would definitely require draining the battery power, hence causing all data in the RAM to be lost similarly as on a PC when it is switched off, which discards the data on the RAM. Therefore, much care and consideration should be given in the acquisition of PDAs that are quite delicate hand-held devices in comparison to PCs.

SUMMARY

In today's fast track life, the cell phone has become the "central station" for most of our electronic, digital or online functions. Even "standard" or "basic" mobile phones, without the seemingly limitless capabilities of the Smartphone, provide useful tools and resources to manage life's increasing digital demands. With such a pivotal role in managing life's complexities, it would be catastrophic if one were to lose his/her phone or, worse, have it stolen! However, a single piece of information, the IMEI number, can protect the owner in such an event and provide invaluable peace of mind. In general, digital hand-held gadgets are reducing

in size and at the same time, they are becoming highly advanced in terms of their feature richness. Criminals also find it lucrative to use the digital hand-held devices for committing crimes. The forensics tools for hand-held devices are as yet, not as advanced as those available for regular computer forensics. The legal community too needs to catch up in terms of understanding and interpreting the digital forensics evidence from hand-held devices. In this chapter, we started with explanation of features of various hand-held devices and explained their forensics aspects along with legal implications.

REVIEW QUESTIONS

1. What is a "hand-held" device? Provide some examples of hand-held devices and explain typically what kind of data is stored on these devices.
2. Do you feel that the advent and proliferation of mobile hand-held devices has influenced the rise in cybercrimes? Support your argument with examples. These could be examples that you have come across in real life or based on what you have been reading and observing.
3. Briefly describe the various cell phone communications standards available today.
4. What is an IMEI number? How does it work to trace a cell phone? What effect do you think it can have on tracking cybercriminals? Provide illustrative situation examples to support your response.
5. Explain the two ways in which PDA forensics tools acquire data. What are the relative advantages and disadvantages?
6. List the various hardware and software components that any typical hand-held device has.
7. In terms of features and functionality, explain the difference between a PDA and a Smartphone.

8. Name some of the popular tools used for the forensics of hand-held devices. For each one, mention the “forensics phase” supported by the tool.
9. Explain why forensics examination of PDAs is more challenging than that of computers.
10. Explain why “printers” should not be precluded from forensics examination in case of a cyber-crime reported.
11. What are some of the common characteristics that a “Smartphone” shares with a “cell phone”?
12. Briefly describe the typical approach taken for iPhone data acquisition.
13. What is a “Jailbroken device”? What are the security implications and possible impact on cybercrime?
14. Explain the challenges faced by investigators when it comes to the forensics of digital camera and digital images.
15. There are a number of hand-held devices explained in this chapter in forensics context. Explain how the BlackBerry device stands apart from those devices from a forensics perspective.
16. What are the “control functions” that a BlackBerry has? How does it help a forensics investigator?
17. In the current milieu of cybercrimes, why do you think forensics of iPods is important?
18. While handling the digital evidence from iPods, what are the key considerations from the legal perspective? Explain by keeping in mind the “chain of evidence” concept.
19. Describe some of the techno-legal challenges involved in collecting evidence from hand-held devices.
20. Explain the difference between computer forensics and electronic discovery.
21. Explain the role of digital forensics in litigations.
22. Explain the key organizational guidelines on cell phone forensics.
23. Based on your reading of this chapter, explain how you see hand-held forensics as a specialized domain and the reasons for it.

REFERENCES

- [1] The following links are for hand-held forensics Paraben Product links:
 Paraben forensics device seizure v3.3 – cell phone forensics product information is available at:
http://www.paraben.com/catalog/product_info.php?products_id=405 (17 April 2010).
 Device Seizure Command Kit – Mobile forensics software and hardware information can be accessed at:
http://www.paraben.com/catalog/product_info.php?products_id=363 (17 April 2010).
 Information about Paraben’s Device Seizure Toolbox is available at:
http://www.paraben.com/catalog/product_info.php?products_id=343 (17 April 2010).
 Information about Device Seizure Field Kit is available at:
http://www.paraben.com/catalog/product_info.php?products_id=501 (17 April 2010).

The pictures of Paraben forensics products and their associated information is available at:

http://www.paraben.com/catalog/product_info.php?products_id=484 (17 April 2010).

Training information about hand-held forensics products is available at:

http://www.paraben.com/catalog/product_info.php?products_id=440 (17 April 2010).

Information about the mobile laboratory kit for hand-held forensics is available at:

http://www.paraben.com/catalog/product_info.php?products_id=490 (17 April 2010).

DS Lite is for analysis and reporting on device seizure and CSI stick case files; information about this product is available at:

http://www.paraben.com/catalog/product_info.php?products_id=482 (17 April 2010).

- [2] Refer to the following link for “3G”: <http://en.wikipedia.org/wiki/3G> (21 April 2010).
- [3] Read the document “*Printing to a Xerox Multifunction Device Using Port 9100*” available at:
<http://www.xerox.com/downloads/usa/en/d/dc00cc0104.pdf> (13 April 2010).
TCP port 9100 Protocol information and Warnings are posted at:
<http://www.auditmypc.com/port/tcp-port-9100.asp> (13 April 2010).
List of TCP and UDP Port Numbers is available at:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (12 April 2010).
- [4] To know about “*Jailbroken*” *iPhones and the Security Risks* associated with them, visit:
http://en.wikipedia.org/wiki/Jailbreaking_for_iPhone_OS (1 May 2010).
<http://www.canada.com/life/Jail+broken+iPhones+hacked+virus/2256956/story.html> (1 May 2010).
http://www.ioltechnology.co.za/article_page.php?iArticleId=5257753 (1 May 2010).
<http://www.networkworld.com/columnists/2009/111109antonopoulos.html> (1 May 2010).
<http://www.reuters.com/article/idUKN2325185820091123> (1 May 2010).
- [5] Documentation about a suite of iPhone Forensics Software Solutions is available at: <http://www.oxygen-forensic.com/en/press/> (18 April 2010). It is the “Oxygen Forensics” suite.
- [6] To know about *BellSouth Intelligent Wireless Network* (mentioned in Section 8.3.8), visit:
<http://www.answers.com/topic/bellsouth-intelligent-wireless-network> (4 May 2010).
<http://encyclopedia2.thefreedictionary.com/Bell+South+Intelligent+Wireless+Network> (4 May 2010).
<http://www.yourdictionary.com/computer/bell-south-intelligent-wireless-network> (4 May 2010).
http://www.rimdev.com/Tutorials/IAS_Descr_Prog_Guide.pdf (4 May 2010).
- [7] The story about use of an Apple iPod by a gang of thieves in England to store information related to their crimes is posted at: http://news.bbc.co.uk/2/hi/uk_news/england/london/3932847.stm (17 April 2010).
- [8] To understand the calibration and standardization aspects to be considered for evaluating digital forensics tools, the paper *Freeware Live Forensics Tools Evaluation and Operation Tips* by Ricci Ieong, Principal Consultant with eWalker Consulting Ltd. can be referred. The paper is available at: <http://www.marcomattiucci.it/ieong.pdf> (22 April 2010).

FURTHER READING

Additional Useful Web References

1. Visit the following link for *Forensics on Yahoo Music* at: <http://new.music.yahoo.com/forensics/> (16 April 2010).
2. You can gain useful information on *Computer Forensics Toolkits, Digital Evidence Software Suites* by visiting:
<http://www.forensics.nl/toolkits> (28 April 2010). There is a short information here on a large number of tools.
3. Check out the following link for links to various forensics toolkits <http://www.filesrecovery.in/file-recovery-tools/pocket-pc-forensic.asp> (25 April 2010).
4. PDA Forensics Tools and Techniques – read about this in the following link (it is a blog). <http://www.informit.com/guides/content.aspx?g=security&seqNum=105&rll=1> (2 March 2010).
5. Pictures and specifications for various *Handheld Digital Forensics Products* can be viewed at: <http://www.dataduplication.co.uk/details/mobilephoneforensics.html> (17 April 2010).
6. Andrew Hoog, Chief Investigative Officer at viaForensics in the US of America is one of the *iPhone forensics experts*. His contact details are quoted below. Phone: +1 312-283-0551 and +1 312-283-0551. The website to contact him is <http://viaforensics.com/contact-us>

7. Read EzineArticles from the Communications: Mobile-Cell-Phone Category at: [http://ezinearticles.com/?Introduction-to-Cell-Phones-and-IMEI-Numbers---What-is-It?-\(Pt1\)&id=4017473](http://ezinearticles.com/?Introduction-to-Cell-Phones-and-IMEI-Numbers---What-is-It?-(Pt1)&id=4017473) (12 April 2010).
8. To know *How to Identify the Cell Phone Number* refer to: http://www.ehow.com/how_5486499_identify-cell-phone-number.html (1 April 2010).
9. The *Importance of the IMEI number for Cell Phone Insurance* can be appreciated by reading the article available at: http://www.ensquared.com/content/No_IMEI_no_insurance_for_unlocked_cell_phones.htm (11 April 2010).
10. Compelson Laboratories – To know more about MOBILedit! Forensic, visit WiKi at: <http://www.forensicswiki.org/wiki/MOBILedit!> (28 September 2010).
11. To know more about Oxygen Software Oxygen Phone Manager II (Forensic version), visit: <http://www.opm2.com/forensic/> (8 October 2006).
12. Paraben Corporation (2006). Paraben Forensics Software, Hardware, and Training, visit the URL at: www.parabenforensics.com/index.html (14 September 2006).
13. How iPhone Unlocking Works can be understood by visiting: http://newsblaze.com/story/20070926073901_chil.nb/topstory.html (1 May 2010).
14. Following are some WCDMA-related links:
 - <http://www.systemdisc.com/wcdma> (20 April 2010).
 - <http://www.wisegeek.com/what-is-wcdma.htm> (20 April 2010).
 - <http://www.topbits.com/wcdma.html> (20 April 2010).
 - <http://www.answers.com/topic/wcdma> (20 April 2010).
 - <http://www.mobileburn.com/definition.jsp?term=WCDMA> (20 April 2010).
 - http://cellphones.about.com/od/cell_phone_glossary/g/wcdma.htm (20 April 2010).
 - <http://www.webopedia.com/TERM/W/WCDMA.html> (20 April 2010).
15. Following are some FOMA Links:
 - <http://www.differencebetween.net/technology/difference-between-wcdma-and-hsdpa/> (20 April 2010).
 - <http://www.mobilemag.com/2004/11/15/ntt-docomo-dual-network-foma-and-lan-voip-phone/> (20 April 2010).
 - http://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol8_1/vol8_1_065en.pdf (20 April 2010).
16. To know about Full Internet Browsing to NTT DoCoMo 3G FOMA™ Handset, refer to: <http://www.3g.co.uk/PR/June2005/1658.htm> (20 April 2010).
17. For an excellent article “*Recovering and Examining Computer Forensic Evidence*,” visit: <http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm> (22 April 2010).
18. Visit the following links accessed between March 2010 and May 2006:
 - For article *Good Practice Guide for Computer based Electronic Evidence*, visit:
http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf
 - For article *Cell Phone Forensic Tools: An Overview and Analysis*, visit:
<http://csrc.nist.gov/publications/nistir/nistir7250.pdf>
 - For article *Toshiba Reports Battery Breakthrough*, visit:
http://news.com.com/206110786_35649141.html?tag=nl
 - For article *Guidelines for the Management of IT Evidence*, visit:
<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf>
 - For article *Best Practice Guidelines for Examination of Digital Evidence*, visit:
<http://www.ioce.org/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf>
 - For article *Guidelines on PDA Forensics*, visit:
<http://csrc.nist.gov/publications/nistpubs/80072/sp80072.pdf>

- For article *Guidelines on Cell Phone Forensics*, visit:
[http://csrc.nist.gov/publications/drafts/
DraftSP800-101.pdf](http://csrc.nist.gov/publications/drafts/DraftSP800-101.pdf)
- For article *Secure Data Erase Utility*, visit:
[http://cmrr.ucsd.edu/people/Hughes/
SecureErase.shtml](http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml) (1 May 2010).
19. There is an informative article by Jesse David Hollington, in which he has described his experience with *review of all the 22 applications that run on a typical iPhone*. To read the article, visit the following link: <http://www.ilounge.com/index.php/articles/comments/iphone-gems-all-22-wallet-apps-reviewed/> (2 May 2010).
20. Read *Why BlackBerry* by visiting: <http://crackberry.com/lecture-1-why-blackberry> (3 May 2010).
21. Learn about advantages of BlackBerry, and BlackBerry FAQs by visiting: http://blackberryfaq.com/index.php?Why_BlackBerry%3F (3 May 2010).
22. The term “probative evidence” is explained at:
<http://legal-dictionary.thefreedictionary.com/probativeness+value> (28 September 2010).
<http://legal-dictionary.thefreedictionary.com/probative> (28 September 2010).
<http://www.answers.com/topic/probative> (28 September 2010).
- Books**
1. Jansen, W. and Ayers, R. (2005) *An overview and analysis of PDA Forensic Tools*, Elsevier.
 2. EC-Council, *Computer Forensics: Investigating Data and Image Files*, EC-Council Press.
 3. Zdziarski, J. (2008) *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets*, O'Reilly Media Inc., USA.
 4. Jones, A. and Valli, C. (2008) *Building a Digital Forensics Laboratory: Establishing and Managing a Successful Facility*, Butterworth-Heinemann publication, USA.
 5. Mart, E.G. (2006) *Getting started in Forensic Psychology Practice: How to Create a Forensic Specialty in your Mental Health Practice*, John Wiley & Sons Inc., USA.
 6. Kubasiak, R.R., Morrissey, S. and Varsalone, J. (2008) *Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit*, Syngress Publishing Inc., USA.
 7. Morrissey, S. (2010) *iPhone Forensic Analysis: A Guide to iPhone and iPod Touch Investigations*, Syngress Publishing Inc., USA.
 8. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Chapter 3), Wiley India, New Delhi.

Articles and Research Papers

1. Use of “Sterile Media” is very crucial for ensuring that cross examination in the court does not bring up questions to raise the “forensic soundness” of the evidence. Therefore, “sanitization” of the media is very important. NIST (National Institute of Standards and Technology) has published a number of guidelines. *NIST guidelines on Media Sanitization* is available at: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf (30 April 2010).
2. There are six excellent articles by Craig Ball. Law students and legal professionals will find a very useful article at: <http://www.almfd.org/pdfs/computer%20forensics%20for%20attorneys.pdf> (26 April 2010).
3. Ayers, R., Jansen, W., Cilleros, N. and Daniellou, R., *Cell Phone Forensic Tools: An Overview and Analysis*, The NIST Report NISTIR 7250 is available at: <http://csrc.nist.gov/publications/nistir/nistir-7250.pdf> (25 December 2009).
4. Sansurooah, K., *An Overview and Examination of Digital PDA Devices under Forensics Toolkits*, the School of Computer and Information Science (SCIS), Edith Cowan University Perth, Western Australia. The paper can be read at: http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/04_Sansurooah%20An%20overview%20and%20examination%20of%20digital%20PDA%20devices%20under%20forensics%20toolkits%20Camera%20Ready%20Paper.pdf (12 April 2010).
5. Frichot, C. *An Analysis of the Integrity of Palm Images Acquired with PDD*, The School of Computer and Information Science, Edith Cowan

- University, Bradford Street, Mt Lawley, Australia. The paper can be read at: http://scissec.scis.ecu.edu.au/conference_proceedings/2004/forensics/Frichot-2.pdf (1 April 2010).
6. Printer forensics using SVM (Support Vector Machine) techniques are discussed at: <http://cobweb.ecn.purdue.edu/~prints/public/papers/nip05-mikkilineni.pdf> (14 April 2010).
 7. Jansen, W.A. *Reference Material for Assessing Forensic SIM Tools*, IEEE National Institute of Standards and Technology, MD 20899, USA and Aurelien Delaitre National Institute of Standards and Technology Gaithersburg, MD 20899, USA, The paper (paper no. ICCST 2007-74) is available at: http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/Reference%20Mat-final-a.pdf (1 April 2010).
 8. Casadei, F., Savoldi, A. and Gubian, P. (2006) Forensics and SIM cards: an overview, *The International Journal of Digital Evidence*, 5 (1). The paper can be accessed at: <http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE3EDD5-0AD1-6086-28804D3C49D798A0.pdf> (20 April 2010).
 9. Breeuwsma, M., de Jongh, M., Klaver, C., van der Knijff, R and Roeloffs, M. (2007) Forensic data recovery from flash memory, *The Small Scale Digital Device Forensics Journal*, 1 (1), The paper can be accessed at: http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf (16 April 2010).
 10. Willassen, S.Y. (2003) Forensics and the GSM mobile telephone system, *The International Journal of Digital Evidence*, 2 (1). It can be found in <http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf> (2 April 2010).
 11. Frichot, C. (2004). *Analysis of the Integrity of Palm Images Acquired with PDD*. Second Australian Computer, Information and Network Forensics Conference. Perth, Western Australia.
 12. Danker, S., Ayers, R. and Mislan, R.P (2009). Hashing techniques for mobile device forensics- *Small Scale Digital Device Forensics Journal*, 3 (1). The paper can be accessed at: http://www.ssddfj.org/papers/SSDDFJ_V3_1_Danker_Ayers_Mislan.pdf (26 April 2010).
 13. Backer, C. Digital Forensics on Small Scale Digital Devices. The article can be accessed at: http://www.crypto.rub.de/imperia/md/content/seminare/itss09/baecker_digital_forensics.pdf (26 April 2010).
 14. Murphey, R. Automated Windows Event Log Forensics – the Science Digest paper is available at: <http://www.dfrws.org/2007/proceedings/p92-murphey.pdf> and CERT-In presentation (28 April 2010)
 15. Sarma, S.S. and Mohorikar, N., *Logs and Forensics*, Department of Information Technology, Ministry of Communications & Information Technology. To know more on this, visit: <http://www.cert-in.org.in/knowledgebase/presentation/Logs-Forensics.pdf> (28 September 2010).
 16. Zdziarski, J. (O'Reilly)'s technical documentation on iPhone Forensics is available at: <http://www.esearchbook.com/files/4/eSearch-Book.1224255173.iPhone%20Forensics.pdf> (2 May 2010).
 17. To understand the risks from "Jailbroken" devices, read the articles available at the following links: "*Jail Broken*" iPhones Hacked by New Virus' (posted November 24, 2009 by Reuters) at: <http://tech2.in.com/india/news/mobile-phones/jail-broken-iphones-hacked-by-new-virus/96752/0> (25 September 2010). In the following link, Reuters has posted another related story:
<http://in.reuters.com/article/idINIndia-44181320091123> (25 September 2010). In the following link, there is an article "*Duh Worm – a new virus targeting "jail broken" iPhones*":
<http://topnews.us/content/28505-duh-worm-new-virus-targeting-jail-broken-iphones> (25 September 2010). In the following link quoted, there is an article "*Apple applies for patent to kill jailbroken devices*":
http://publication.samachar.com/pub_article.php?id=9905908&nextids=9908717|9907847

|9907654|9905907|9905908&nextIndex=0
(25 September 2010).

18. To understand about “probative value of evidence,” you can refer to the paper by Deborah Davis and William C. Follette (2002) Rethinking the probative value of evidence: Base rates, intuitive profiling, and the postdiction of behavior, *Law and Human Behaviour*, 26(2). The article is accessible at: <http://www.sierratrialandopinion.com/papers/Probativevalue1.pdf> (28 Sept 2010).
19. Regarding Cell Phones without IMEI number (mentioned in Box 8.4) refer to the article at: http://www.dnaindia.com/mumbai/report_phones-without-imei-numbers-to-be-disconnected-from-tomorrow_1318381 (17th December 2010).

Video Clips

1. iPhone Forensics Demo is available at: <http://www.youtube.com/watch?v=op-HyBVN2Ek> (15 April 2010).
2. To know more about iPhone and its hardware components, visit:
http://www.youtube.com/watch?v=mPhciMud0MM&feature=player_embedded (1 May 2010). It is a video clip that shows the *Insides of Apple iPhone* through the exercise of opening one iPhone handset.
For a closer look at the iPhone, visit:
<http://www.youtube.com/watch?v=YgW7or1TuFk&NR=1&feature=fvwp> (1 May 2010).
To learn how to use an iPhone, you can visit the video clip available at:

http://www.youtube.com/watch?v=s_f-KK140vM&NR=1 (1 May 2010).

3. A demo of Mobile Recovery System can be seen at: <http://www.youtube.com/watch?v=25eBn9N20C4> (12 April 2010).
4. *Cell Phone SIM Card Spy: Spy On A Cellphone* can be seen at: http://www.youtube.com/watch?v=iUkJIO_GgsqM&NR=1 (10 April 2010).
5. Learn how a cell phone can be intercepted at: http://www.youtube.com/watch?v=W28SOiZ_-8c&NR=1 (11 April 2010).
6. Learn how to track a cell phone by SMS by visiting: <http://www.youtube.com/watch?v=WWBfovRI15k&NR=1> (11 April 2010).
7. A short video clip on how to locate a mobile phone is available at: <http://www.youtube.com/watch?v=QzwT1UNWYOk&NR=1> (9 May 2010).
8. A video demo of iPhone forensics demo can be accessed at: <http://oreilly.com/catalog/9780596153595> (18 April 2010).
9. How *Mobile Cell Phone Number Tracking Tracing* is done can be seen through a video clip (especially for locating small children who move with a mobile phone) at: <http://www.youtube.com/watch?v=hZKfNRxdUeI&feature=related> (13 April 2010).
10. *Cost of Forensics* is explained in the video clip in the following link:
<http://www.youtube.com/watch?v=ZywiP4l3ee4> (14 April 2010).

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, C, D, F, G, H, I. These are provided in the companion CD.

9 | Cybersecurity: Organizational Implications

Learning Objectives

After reading this chapter, you will able to:

- Learn about the top web threats faced by organizations.
 - Understand what is “social computing” and why organizations should be careful about it.
 - Understanding the risks associated with “social media networking.”
 - Understand Intellectual Property Right (IPR)-related offenses; especially about the implications of “software piracy” which is one of the IPR crime.
 - Understand “cloud computing” challenges for organizations.
 - Learn about data privacy and security best practices essential for organizations.
 - Appreciate the importance of “forensics readiness”.
 - Understand the guidelines for computer and Internet usage as well as the guidelines for safe computing.
 - Learn about importance of “media and asset protection” in organizations.
 - Appreciate “endpoint security” in organizations.
 - Appreciate the importance of “incidence management systems”.
 - Consolidate your understanding about regulatory framework for cybersecurity.
-

9.1 Introduction

In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices or intense scans from criminal groups. To understand the relevant aspects of cybercrimes in perspective, refer to Fig. 9.1 (it is the same as Fig. 6.1 in Chapter 6).



The examples, mini cases and illustrations in Chapter 11 (in CD) are the extended material for this chapter.

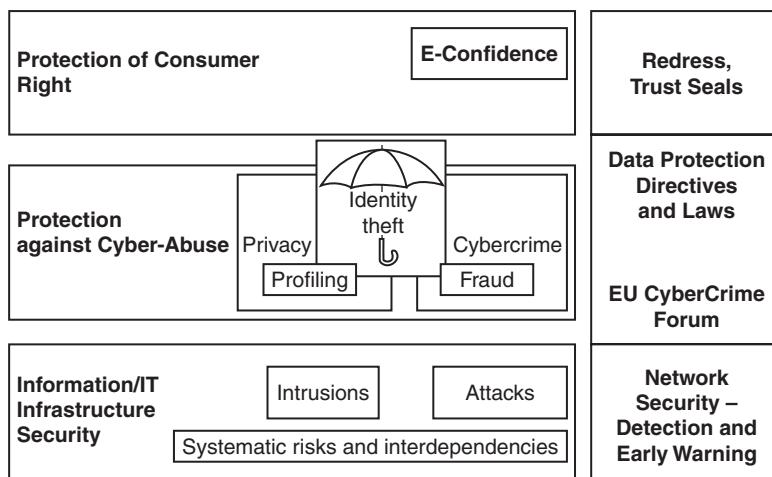


Figure 9.1 | A cybersecurity perspective. EU is the European Union.

Note the two examples in Chapter 11 (in CD) – Examples 10 and 11 in Section 11.2. Example 10 shows real-life situation of Internet frauds that include cases of fraudulent withdrawal of money from banks through Internet/online banking. Example 11 concerning infinity e-Search BPO case brings out the point that Indian BPO organizations have implications from the Indian IT Act.

There are “security challenges with mobile workforce” – see the presentation made in a conference held in December 2009.^[1] Besides these examples, there are many illustrations about how organizations are endangered today, not to forget the insider threats. Authors’ experience in the industry as well as literature survey shows that such threats are large (see Fig. 9.2).

A “security breach” is defined as unauthorized acquisition of data that compromises security, confidentiality or integrity of personal information (PI) maintained by us. However, good faith acquisition of PI either by an employee or an agent of an organization for business purposes is not considered to be a breach, provided that the PI is not used or subjected to further unauthorized disclosure.



PI is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Most information the organization collects about an individual is likely to come under “PI” category if it can be attributed to an individual. For an example, PI is an individual’s first name or first initial and last name in combination with any of the following data:

1. Social security number (SSN)/social insurance number.
2. Driver’s license number or identification card number.
3. Bank account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual’s financial account.



Figure 9.2 | Insider threat scenario (2000–2009).

4. Home address or E-Mail address.
5. Medical or health information.



An insider threat is defined as “the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other ‘trusted’ individuals.”

Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of “insiders” such as:

1. A *malicious insider* is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrity and/or availability.

2. A *careless insider* can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.
3. A *tricked insider* is a person who is “tricked” into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via “pretexting” (known as social engineering).

9.1.1 Insider Attack Example 1: Heartland Payment System Fraud

A case in point is the infamous “Heartland Payment System Fraud” that was uncovered in January 2010. This incident brings out the glaring point about seriousness of “insider attacks.” In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is transmitted through a payment network. In this case, a piece of malicious software (malware, i.e., a “keystroke logger”) planted on the company’s payment processing network, recorded payment card data as it was being sent for processing to Heartland by thousands of the company’s retail clients. Digital information within the magnetic stripe on the back of credit and debit cards was copied by keylogger (this tool was mentioned and explained in Chapter 2). Perpetrators created counterfeit credit cards. Unfortunately, these “break-ins” went undetected for nearly 6 months. Visa temporarily declared Heartland to be PCI-DSS non-compliant; PCI-DSS is Payment Card Industry Data Security Standard. Refer to Chapter 11 for case illustrations on credit card-related frauds (see Section 11.4.2).

9.1.2 Insider Attack Example 2: Blue Shield Blue Cross (BCBS)

Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 – the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private information of approximately 500,000 customers at risk in at least 32 states. Readers interested to know more on this can visit http://en.wikipedia.org/wiki/Blue_Cross_Blue_Shield_Association. The hard drives containing 1.3 million audio files and 300,000 video files related to coordination of care and eligibility telephone calls from providers and members were reportedly stolen from a leased office. Three hard drives ($3.5'' \times 10''$) were physically removed from server racks on computers inside data storage closet at a training center. Incidences such as these bring out glaring point about physical security weakness at organizations. The two lessons to be learnt from this are:

1. Physical security is very important.
2. Insider threats cannot be ignored.

What makes matters worse is that the groups/agencies/entities connected with cybercrimes are all linked (see Fig. 9.3).

There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc. to name a few.

Over a period of time, security threats to organizations have morphed from simple ones to very sophisticated ones (refer to Fig. 9.4). The number of security attacks as well as their sophistication and variety rose from the 1980s and onward; this is in line with the sophistication of cybercriminals over a period of time (see Fig. 7.21 in Chapter 7).

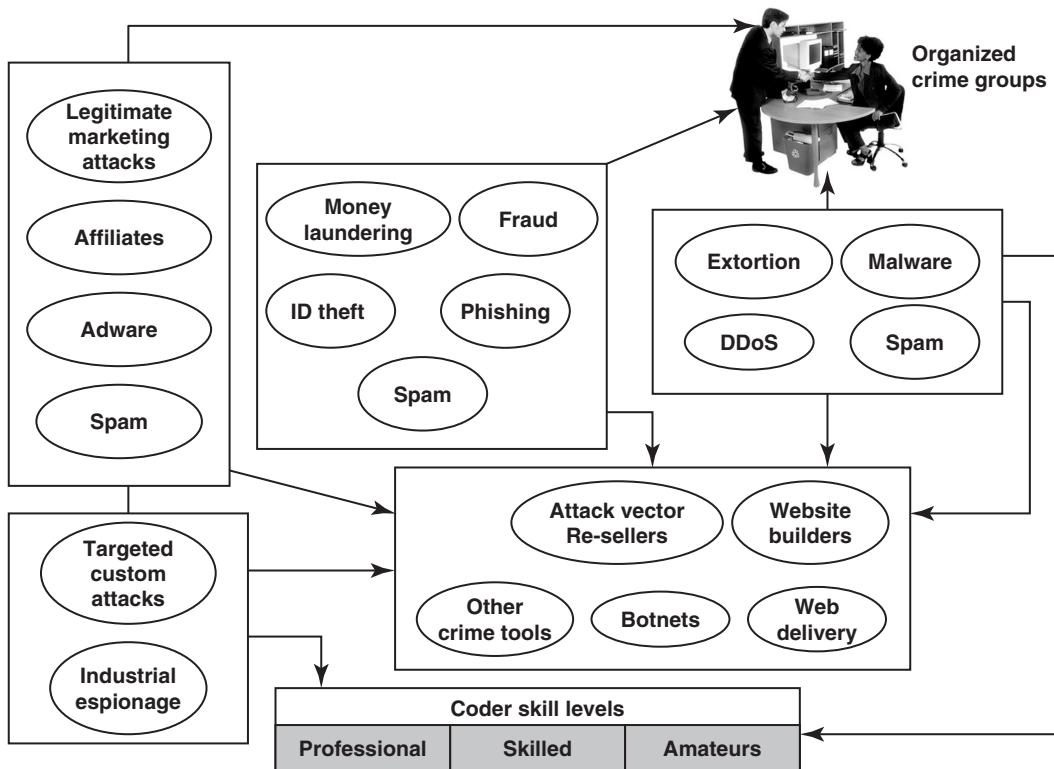


Figure 9.3 | Cybercrimes – the flow and connections.



A key message from this discussion is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cybersecurity practices and “privacy” which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

- 1. Informational/data privacy:** It is about data protection, and the users' rights to determine how, when and to what extent information about them is communicated to other parties. The execution of this right may be based upon their knowledge about what the other party's intention is.
- 2. Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.
- 3. Communication privacy:** This is as in networks, where encryption of data being transmitted is important.
- 4. Territorial privacy:** It is about protecting users' property – for example, the user devices – from being invaded by undesired content such as SMS or E-Mail/Spam messages. The paradigm shift in computing brings many challenges for organizations; some such key challenges are described here. Refer to Chapter 1 for examples of defacement of websites.

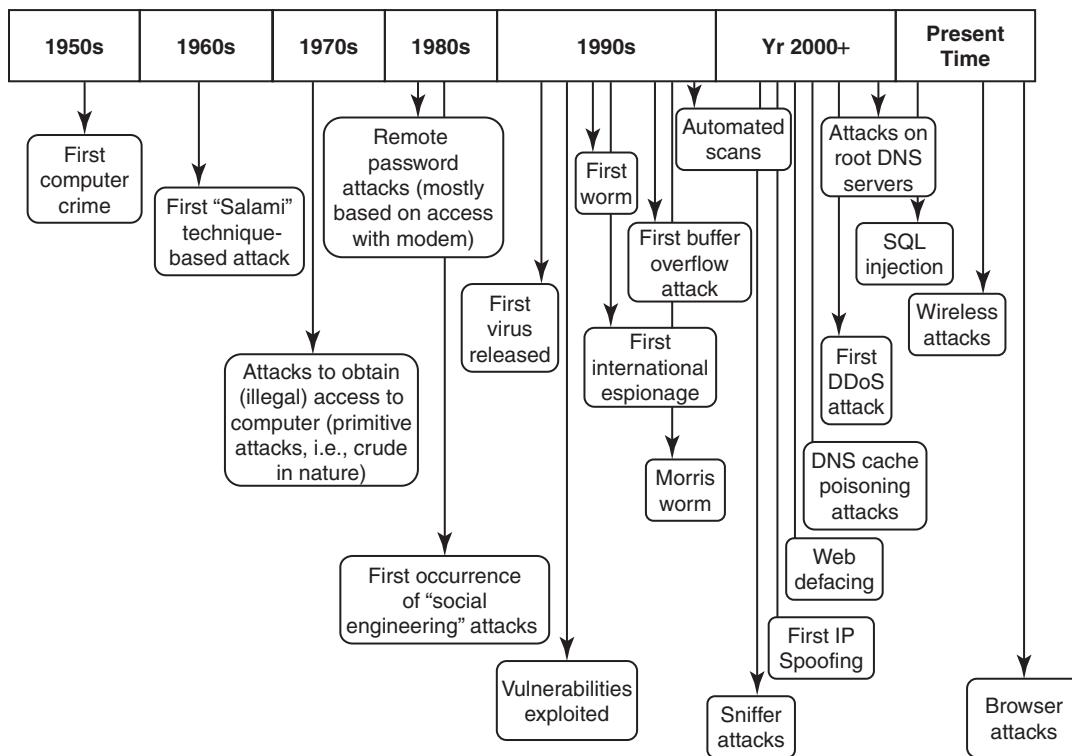


Figure 9.4 | Security threats – paradigm shift.

The key challenges from emerging new information threats to organizations are as follows:

1. **Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website. For example, suppose your competitor's networks, using their firewalls and intrusion detection system (IDS) detect a large amount of traffic coming from your IP to their product page, then they may conclude that your organization is planning to come out with a similar product. This may make them take an anticipative action in counter by launching a new promotion to thwart the impact of your new product campaign! Refer to Fig. 9.3 (there is "industrial espionage" block mentioned in bottom left of that figure).
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names. For example, given the industrial espionage activities that are rampant these days, your marketing research team may be blocked from accessing your competitor's website, thus, limiting the marking team's ability to conduct industry and competitive intelligence for your firm.
3. **IP-based "cloaking":** Businesses are global in nature and economies are interconnected. There are websites that change their online content depending on a user's IP address or user's geographic location. For example, let us say your competitor web tool recognizes one of your technical employees surfing its site and displays incorrect or inaccurate product information to your IP address, thus, making it impossible to obtain accurate competitive information.

4. **Cyberterrorism:** This term was introduced and explained in Chapter 1 (Box 1.1). “Cyberterrorism” refers to the direct intervention of a threat source toward your organization’s website. One example of this occurred in year 1997, wherein the Pentagon simulated a cyberattack. Through this simulation, they found that attackers were using ordinary computers and widely available software that could disrupt military communications, electrical power and 9-1-1 networks in several cities in the US. Since then, hacking tools and expertise have become only more widespread.
5. **Confidential information leakage:** “Insider attacks” are the worst ones (refer to Fig. 9.2). Typically, an organization is protected from external threats by your firewall and antivirus solutions. However, an organization is not protected from the internal threats that occur everyday when employees surf the Internet and inadvertently give out confidential information over time. Your competitor can determine your strategic initiatives, such as a hostile takeover, based on the information that your employees pull from their website.

There is a link quoted in References about “Top 5 Insider Attacks of 2009.”^[2] In that link, there is an MP3 audio through which you can hear the views of experts about insider attacks including the infamous “identity theft.”

9.2 Cost of Cybercrimes and IPR Issues: Lessons for Organizations

Reflecting on the discussion in the previous sections brings us to the point that cybercrimes cost a lot to organizations (see Fig. 9.5).

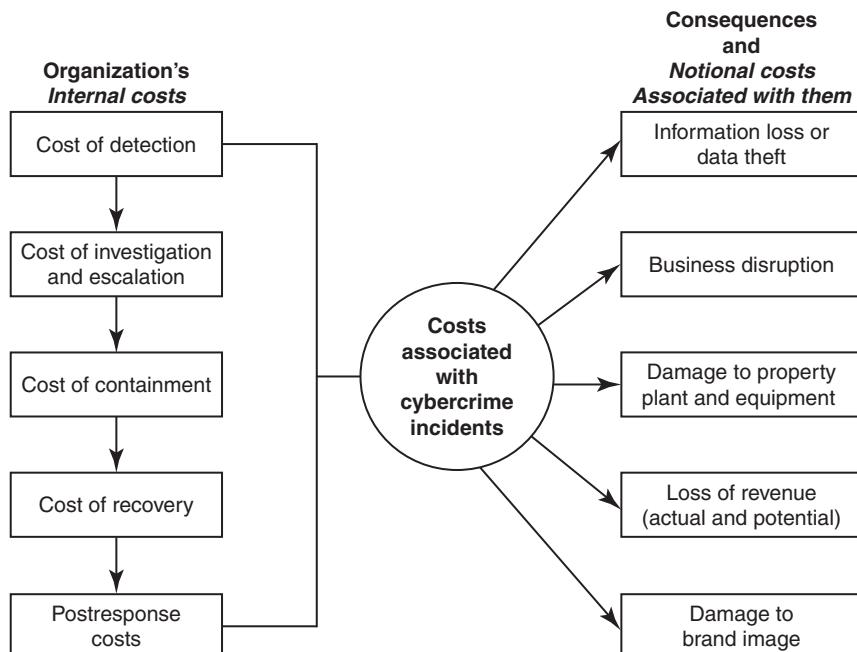


Figure 9.5 | Cost of cybercrimes.



When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

Detection and recovery constitute a very large percentage of internal costs. This is supported by a benchmark study conducted by Ponemon Institute USA carried out with the sample of 45 organizations representing more than 10 sectors and each with a head count of at least 500 employees. In this benchmark study, they found that the total annualized cost of cybercrime for the sampled organizations ranged from a low of US\$ 1 million to nearly US\$ 532 million. Trade secret or Intellectual Property (IP), when it leaves the organization, is considered as one of the biggest impacts of cybercrime. The benchmark study also showed that there are high costs associated with Malicious Code, viruses, webattacks and attacks by malicious insiders. It is the (a) “frequency of cybercrimes” along with (b) its success (i.e., cyberattacks that get through organization’s firewalls and IDS) together that become a key reason for organizations to worry about the “cost of cybercrimes.” “Information theft” represents the highest external cost. There are cyber-criminal syndicates today!

9.2.1 Organizations have Internal Costs Associated with Cybersecurity Incidents

The internal costs (see Fig. 9.5) typically involve people costs, overhead costs and productivity losses. The internal costs, shown in Fig. 9.5, are in order from largest to the lowest and that has been supported by the benchmark study mentioned previously:

1. Detection costs (25% – largest).
2. Recovery costs (21%).
3. Postresponse costs (19%).
4. Investigation costs (14%).
5. Costs of escalation and incident management (12%).
6. Cost of containment (9% – lowest).

Refer to “attack vector” explained in Section 2.7 of Chapter 2 – this term is used to categorize an attack type. The cost of cybercrime varies depending on the attack type, industry type and organizational size. For example, the financial and defense sectors worldwide have attracted more cyberattacks than any other industry. This is not surprising, considering the nature of data held by the organizations in these sectors. An important question for an organization is “how effective is our security posture?” This makes sense with the distribution of the cybercrime costs mentioned above. For example, a CEO of an organization would like to focus on tools and automated methods to get better at detecting cybercrimes. Any tool that detects smartly would be on the CEO’s shopping list!

The consequences of cybercrimes and their associated costs, mentioned in Fig. 9.5, show a pattern (a benchmark study supported this):

1. Information loss/data theft (highest – 42%).
2. Business disruption (22%).
3. Damages to equipment, plant and property (13%).
4. Loss of revenue and brand tarnishing (13%).
5. Other costs (10%).

There is a subjective element depending on the nature of an organization – for example, revenue costs could be higher for a fully E-Commerce company that purely sells from the Web-based portal. Suppose that portal is completely down following a cyberattack. Under those circumstances, data that is of IP type (e.g., design documents), business confidential information (such as key customer list, organization's classified information etc.) would be more harmful to lose compared to PI about people and their families, that is, all the personal information and sensitive personal information (PI/SPI) that could be lost/stolen due to cyberattacks.

The benchmark study mentioned at the beginning of this section revealed that the percentage of organizations impacted by various types of cybercrimes show the following distribution:

1. Viruses, worms and Trojans (100%): To know more on these refer to Section 4.6 and Figs. 4.1–4.3 in Chapter 4.
2. Malware (80%): For detail discussion on this refer to Box 4.3 and to know more on “SQL injection” refer to Section 4.10.
3. Botnets (73%): Refer to Section 2.6 and Figure 2.8.
4. Web-based attacks (53%): Refer to the discussion in Section 9.3.
5. Phishing and social engineering (47%): Refer to Chapters 4 and 5, and the discussion in the introduction section of this chapter. Also refer to Section 2.3.1, Chapter 2.
6. Stolen devices (36%): Refer to Section 3.9.3 and tips to secure your cell/mobile phone from being stolen/lost in Box 3.6.
7. Malicious insiders (29%): Refer to Fig. 9.2.
8. Malicious Code (27%): Refer to Chapters 2 and 4.

When the data for “average days taken to resolve cyberattacks” was formulated according to the cyberattack categories, the following emerged as the picture (in the benchmark study mentioned earlier):

1. Attacks by malicious insiders (42 days – highest).
2. Malicious Code (39 days).
3. Web-based attacks (19 days).
4. Data loss due to stolen devices (10 days).
5. Phishing and social engineering attacks (9 days).
6. Viruses, worms and Trojans (2.5 days).
7. Malware (2 days).
8. Botnets (2 days).



There are many new endpoints in today's complex networks; they include hand-held devices.

Again, there are lessons to learn:

1. **Endpoint protection:** It is an often ignored area but it is important (this aspect of security is explained in Section 9.12). IP-based printers, although they are passive devices, are also one of the endpoints. Printers are no more just dump devices especially in the network printer era. Many organizations, which otherwise have reasonably good security practices, tend to completely neglect their network printers – refer to discussion in Section 8.3.3 of Chapter 8.
2. **Secure coding:** These practices are important because they are a good mitigation control to protect organizations from “Malicious Code” inside business applications (especially those applications that are mission critical). Refer to Fig. 9.21 and also to Ref. #5, Books, Further Reading.

3. **HR checks:** These are important prior to employment as well as after employment (from malicious insiders' considerations).
4. **Access controls:** These are *always* important, for example, shared IDs and shared laptops are dangerous. Access privileges should be granted carefully, especially when they involve access to confidential and sensitive information of the organization (refer to Ref. #7, Books, Further Reading). In the benchmark study mentioned earlier, it was found that there was a direct positive correlation between the amount of money organizations spent and the cybercrimes prevented/minimized in the long run.
5. **Importance of security governance:** It cannot be ignored – policies, procedures and their effective implementation cannot be over-emphasized. For a detailed discussion, refer to Ref. #8, Books, Further Reading. Good governance is essential for maintaining a healthy security posture in the organization. Ultimately it helps to reduce cybercrime incidents.

9.2.2 Organizational Implications of Software Piracy



Use of pirated software is a major risk area for organizations.

From a legal standpoint, software piracy is an IPR violation crime. Use of pirated software increases serious threats and risks of cybercrime and computer security when it comes to legal liability; violation of copyright laws (pirated software) makes company officials criminally liable under the Copyright Act (see Appendix T in CD); and “knowing use” is also a criminal offense under the Act. Use of unlicensed software, that is, pirated software, should be discouraged in the organization. One of the lapses exploited by cybercriminals is the vulnerability of nongenuine computer software. One example is the recent global spread of the Conficker virus (refer to Table 4.8 in Chapter 4). The spread of this virus can be partly attributed to the lack of automatic security updates for unlicensed software. As per report posted at <http://trak.in/tags/business/2010/05/12/software-piracy-india>, India's rank is 9 in the 2009 list of top countries in piracy. In the past, the 2006 study by IDC found that 29% of websites and 61% of peer-to-peer sites offering pirated software tried to infect test computers with “Trojans,” Spyware, keyloggers and other tools of identity theft.

For year 2009, it was estimated that by reducing piracy rate by 10% by 2009, India had the potential for adding 115,000 new jobs in the IT industry. Non-genuine software can potentially disrupt smooth functioning of an organization's operations by adversely affecting the system security infrastructure (see Fig. 9.6). The most often quoted reasons by employees, for use of pirated software, are as follows:

1. Pirated software is cheaper and more readily available.
2. Many others use pirated software anyways.
3. Latest versions are available faster when pirated software is used.

Notwithstanding these excuses, organizations should track software licenses to ensure that only genuine copies are used and that the number of installations is not more than the allowed number. It is possible to do this by establishing a software license tracker tool. Organizations that ignore the issue of pirated software could be exposing themselves to security risks, with implications such as loss of data, confidentiality, integrity, and reduced operational performance. Indirect threats of deploying non-genuine software include increased cost of protection, remediation and also a possibility of the organization/user becoming a part of a larger nexus of antisocial elements funding illegal software businesses and contributing to the network of organized crime (see Figure 9.3).

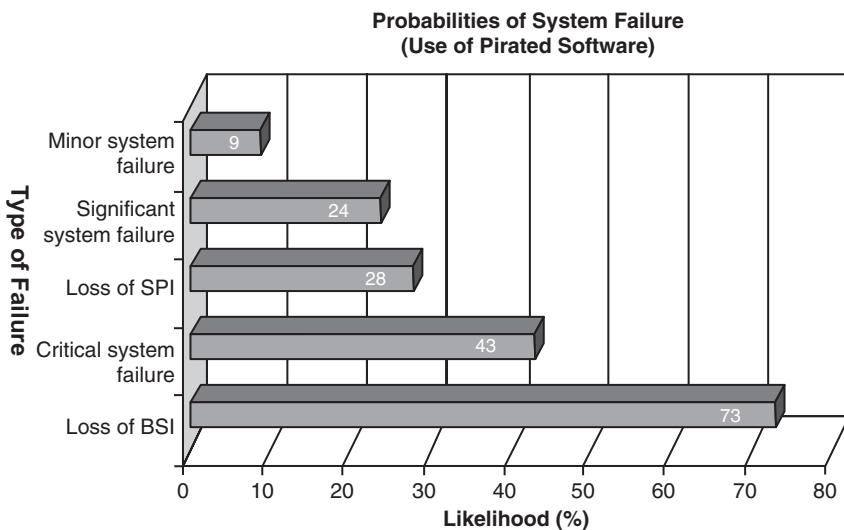


Figure 9.6 | Probabilities of system failure (use of pirated software).
SPI is sensitive personal data and BSI is business sensitive information.

9.3 Web Threats for Organizations: The Evils and Perils

Internet and the Web is the way of working today in the interconnected digital economy. More and more business applications are web based, especially with the growing adoption of cloud computing (refer to Chapter 2 – Section 2.8 for discussion on cloud computing). There are web portals too in the E-Commerce model of doing business. Video and audio contents are delivered from the Web; software and infrastructure get delivered from the cloud! There is an inevitable dependence on the Internet (weather forecasts, stock trading and video conferencing). Therefore, cybercriminals find it convenient to use the Net for committing crimes. Let us understand the web threats for organizations today in this paradigm.

9.3.1 Overview of Web Threats to Organizations

The Internet has engulfed us! Large number of companies as well as individuals have a connection to the Internet. Employees expect to have Internet access at work just like they do at home. *Mobility* is picking up in India too though at a much limited pace compared to other countries. Mobile workforce has various categories (see Box 9.1). Workforce mobility poses challenges for IT managers whose agenda is to protect the business and business assets against malware (recall the discussion in Section 9.2). Protection of information assets is important; especially protection of removable/detachable media. For a detail discussion about this refer to Ref. #11, Books, Further Reading. Other concerns are about keeping Internet bandwidth available for legitimate business needs and ensuring uptime of applications and business websites. (Recall the discussion about DoS attacks, man-in-the-middle attacks in Chapter 4.)



IT managers must also find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

Box 9.1 Mobile Workforce – Category of “Remote Workers”

Following are various types of mobile workers/remote workers:

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes homeworkers, telecottagers, and in some cases, branch workers.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in hotel rooms and other semitethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. **Road warrior:** This is the ultimate mobile user; such a remote worker spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit, or in hotels. This type includes the sales and field forces.

There is another way, too, for classifying the workforce:

1. **Office-based mobile workers:** These are the ones who spend most of their time in a company-provided office, but they also sometimes work at home or in a third place.
2. **Non-office-based mobile workers:** These are the ones in the field, such as a salesperson, or workers between buildings on a corporate campus, such as IT professionals. They are more often at someone else's office than their own.
3. **Home-based mobile workers:** These are the former telecommuter; this employee class spends most of the week working in a home office, but comes into the corporate workplace for meetings or collaborative work sessions.

From an organizational perspective, web threats can be classified into two broad categories. First, employees do a number of activities online such as visiting infected websites, accessing pornographic sites, responding to Spam mails (refer to Chapter 11 in CD for case illustration on this) and attempting to hack sites (for legitimate and illegitimate reasons) to name a few. Second, there are many challenges and difficulties IT managers face when it comes to managing web use in a secure and efficient way and when it comes to handle an “incident” alert received. IT management is preoccupied with some of the top issues – they are described below:

1. Employees wasting time on social networking and similar sites (such as Facebook, Twitter, etc.) and its impact on employee productivity. With rise in workforce mobility,^[1] this is likely to affect even more as it is very difficult to monitor remote employee. This threat is more in the case of younger employees; especially in the IT industry where at times they are on the bench.
2. Enforcing “Acceptable Use Policies” is a challenge, especially, in very large, multi-location and matrix-structured organizations where getting the leaders to agree are a big challenge.
3. The difficulty in monitoring employees’ web usage – there are tethered as well as remote employees (see Box 9.1); keeping them under watch constantly is next to impossible. Also, people are becoming increasingly aware about their “privacy rights.”
4. Keeping security systems up to date with patches and signatures is a challenge; this includes the challenge of operating system (OS) patches as well. We often hear about Microsoft vulnerability attacks. Most of us are busy installing one patch or the other on our laptops or desktops – it is the necessary evil in Windows world.
5. Legal and regulatory compliance risks (such as employees visiting inappropriate websites and the accidental disclosure of confidential information online). Laws are getting tough and regulatory compliance pressures are high especially in data breaches and employee privacy matters.

6. Keeping the Internet bandwidth free for legitimate business use – there are bandwidth-hungry applications such as live video conferencing, YouTube, online training modules, as class room-based faculty delivered face-to-face training is the thing of the past, etc.
7. Protecting remote workers and homeworkers (workforce mobility) – mobility of white collar workers is on the rise as mentioned (see Box 9.1).
8. Employees using unauthorized Web-based applications – this is indeed a challenge in a virtual team environment with employees spread across locations.
9. Protecting the organization against Spyware and malware – recall the discussions in Chapters 2–4. Today there are tools from Websense Inc., called Websense Enterprise Edition, meant for content filtering. Remote filtering capabilities are incorporated into the newest versions of Websense. Web filtering and web security software restrict the use of Internet. In References, some useful links are provided for those who are interested in exploring the features of this tool.^[3]
10. Protecting multiple offices and locations – these are effects of globalization and the emerging “follow-the-sun-model” wherein business never sleeps and customers’ insistence on business continuity means that there are alternate locations acting as shadow sites.

Thus, the worldwide web or the “Web,” as it is commonly known, is a fantastic business resource; however, without proper protection and management it is also a source of danger and unnecessary expense for all businesses (irrespective of size). Organizations need not be hapless about handling these challenges to mitigate the associated risks for each of these challenges.

Employee Time Wasted on Internet Surfing

This is a very sensitive topic indeed, especially in organizations that claim to have a “liberal culture.” Some managers believe that it is crucial in today’s business world to have the finger on the pulse of your employees. They believe that by monitoring employees you can have all the information you need for making informed decisions. However, an action led by this thought can be tricky. Imagine the challenges; let us say that one employee is working very hard while another employee just keeps surfing the Net for hours. Even when you observe this first hand, it is difficult to prove what one employee says about another unless you are right there to see what is happening. If you challenge the employee surfing Net then it can harbor resentment and ill feeling between employees.



People seem to spend approximately 45–60 minutes each working day on personal web surfing at work.

Organizations need to discipline an employee for Internet misuse. One way of doing that is through “Safe Computing Guidelines/Internet Usage Guidelines” (discussed in Section 9.8). However, these guidelines alone are not enough. Organizations need software tools, which, once installed, monitor employee Internet activities in the background. Cookies store the surfing activities (see Box 9.2).

Employees wasting time online is a big issue for most organizations and at the same time the ways for complaining about it are getting limited. Take for example the developers; they have so many online groups and communities in the development network (e.g., the MSDN – Microsoft Development Network) that they need to refer. There are also blogs posted on the topic of bugs, numerous problems associated with software development, platform specific tips, etc. It is hard to challenge who is using the Web during work hours for personal reasons and who is using it in context of the task assigned. “Policing” employees is just

Box 9.2 Cookies and Internet Activities

Let us understand what a "cookie" is. Cookies are pieces of information that get passed to your browser by a server on the Internet. They get stored on your hard drive and are returned to the server when requested. Of course the information, that is, the cookie is not placed on your hard drive for general distribution. Although a server sets a cookie, the browser will not give up that cookie data to another server. However, the exchange of data does allow the server to set cookies to keep track of information about your preferences that is potentially useful to you and to the server operator.

Cookies come in two types: (a) session cookies and (b) persistent cookies. A "session cookie" is also called as "transient cookie." It lasts only for the duration of the Internet session, that is, it is not "persistent." Session cookie is not retained after the browser is closed – it is stored in temporary memory. From "privacy" perspective, session cookies can be considered to be safer because they do not collect information from the user's computer. Typically, session cookies will store information in the form of a session identification that does not personally identify the user. This is not the case with "persistent cookies." As the name implies, a "persistent cookie" lasts beyond the browser session. The other name for persistent cookies is "stored cookie." A persistent cookie gets stored on a user's hard drive until it expires or until the user deletes the cookie; they are set with expiration dates and are used to collect identifying information about the user, such as web surfing behavior or user preferences for a specific website.

We may never think about this but it is a reality – our web browser usage can be tracked. A "cookie" is a text file placed on a user's computer by a website to help track that user's browsing activities. Only a few Internet users are aware that they can set their browsers to reject cookies. For example, the Internet Explorer browser in its version 8 (IE8) has the option "InPrivate" browsing whereby new cookies become "session cookies." IE8 has also got another feature "InPrivate blocking" whereby it keeps track of where you see third-party content and starts blocking once it sees at more than 10 sites. Thus, it blocks cookies and other types of third-party contents. Cookie-blocking feature is also available with Firefox – users can reject all cookies or third-party cookies or add exceptions. Users can turn cookies into session cookies.

Often people ask "are cookies bad?" Well, people know that eating too many cookies is bad for health! What about the infamous "Internet cookies?" Of late, the use of cookies has become a fairly controversial topic. Some people strongly believe that they are invasion into their privacy, while some believe they are boon to effective browsing with the Internet! Unfortunately, there are no reliable figures available to know how many websites install cookies. Some cookies track the activities of a user at a particular website whereas others can track the user from website to website.

It is alleged that although cookies were not designed for the purpose of impacting people's privacy, in reality it is turning out to be so. For example, in the US, it was found that the Federal Office of National Drug Control Policy (the so-called "drug czar's" office) was using cookies to track web surfers' drug-related information requests. This raised a storm of criticism as it was believed that such use of cookies might enable drug czar's office to secretly record people's online activities. Eventually, the Federal Office of Management and Budget banned the use of cookies on Federal Government websites.

Microsoft announced new third-party cookie controls for Internet Explorer, actively warning consumers and allowing them to reject cookies, which could be used to track their activities all across the Web. Advertisers exploit cookies to their marketing advantage – cookies become more pervasive, and as advertisers are able to track more and more of people's web preferences, the issue of privacy is driven further to the fore. At the following link there is an interesting information if the government would know what websites you visit:

<http://computer.howstuffworks.com/government-see-website2.htm> (12 August 2010).

next to impossible; employees may raise "privacy" objections about it saying they are being treated as the "fish-in-the-glass bowl"!

Mindless and objective-less surfing on the Internet seems to be a "disease" that is spreading. If not controlled, it can be very time wasting and can reduce employee productivity. There are also other problems associated with excessive web surfing, it keeps the bandwidth under usage continuously; imagine thousands

of employees of a single organization utilizing the bandwidth and its possible impact on other honest workers who need to use the Internet for official work-related activities; they end up getting only the slack time! Monitoring does keep the IT department very busy because dealing with the disciplinary issues is a serious drain on management time – first, you have to constantly monitor; then you have to classify the findings and then you have to report. Second, you need to hold meetings to discuss the issues; then you need to agree on an action plan and finally you need to report the actions taken. Moreover, the IT department (or whichever is the department to whom the task is assigned) is expected to do this on an ongoing basis. Therefore, the IT department or whichever department is given the task of monitoring employees' Internet surfing time needs to be empowered with the ability to restrict access to non-work websites. Without this kind of technology, employee's time wasting goes unchecked and policy enforcement becomes much more difficult. Indeed seamless tools are required for this. One such tool that we are aware of is the MessageLabs Security SafeGuard tool. Information about this tool can be found by visiting www.messagelabs.com. According to our experience, this solution lets you set and apply consistent policies that restrict access to different categories of website. However, organizations may like to take a more permissive approach and accept that a certain amount of personal Internet use is acceptable; indeed, as mentioned before, because of "privacy" expectations and other expectations that employees have. Many employees (prospective as well as those who are engaged with an organization) now see "Internet Surfing as a right!" Therefore, a tool like MessageLabs Security SafeGuard lets you apply time and bandwidth limits on use so that people can have access but within reasonable boundaries.

Enforcing Policy Usage in the Organization

Figure 9.7 depicts the policy hierarchy chart. An organization has various types of policies. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization.

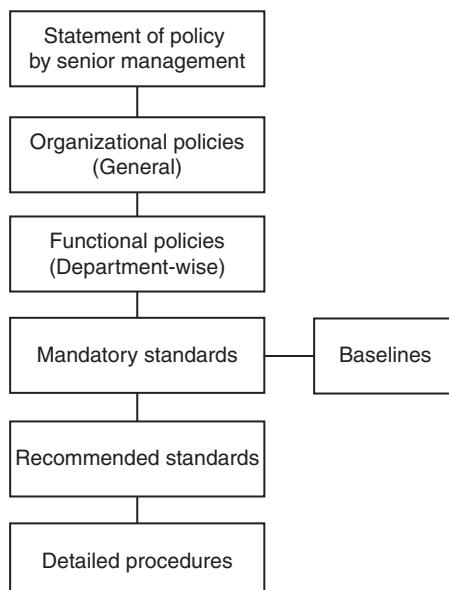


Figure 9.7 | Policy hierarchy chart.

Box 9.3 Cookies – Where Did They Come From?

Most computer-related terms are interesting! Some people believe that the term cookie comes from the story *Hansel and Gretel* - both were afraid that they would get lost in the forest and so they marked their trail through a forest by regularly dropping crumbs along their path. Of course, Hansel and Gretel used bright stones, not cookies to mark their trail; nonetheless, the legend persists. You must have heard the term "privacy policy." All privacy-aware organizations post their privacy policies on their website and in prominently visible way which is privacy best practice in terms of website design. The privacy policy must clearly state whether the site uses any cookies and if so, for what type of use, what kind of information is stored in those cookies when users visit the organization website and for how long that information is stored. Also for what purpose the visitor's information will be used must be clearly stated. Have you ever thought how "cookies" came into existence?

In 1994, Netscape created cookies as a special browser feature. Netscape did that to make Internet browsers' life easier while surfing on the Web. The concept behind a cookie is similar to that of a computer's preferences file, that is, to keep track of how the user wants a site to look or function. The idea was to make it a one-time task. Once the preferences are set, the user does not have to input routine information upon each visit. Cookie creators thought it would be especially useful in enabling "shopping cart" services on websites. It was meant to allow consumers to click from page to page choosing items to buy, while a virtual clerk kept track of the items until the consumer was ready to check out. Cookies also allowed a site owner to observe which displays attracted the consumer's attention and which needed some sprucing up. Netscape did not initially inform consumers about the clandestine activity on their hard drives and probably did not foresee the firestorm that would follow! They obviously did not imagine the shape of the things to come afterward!

Eventually, the Cookie technology was reported by media in January 1996. Public pressure mounted and Netscape added a tool to disable cookies for the next version of their web browsing software. However, it was not easy to do the disabling! Website users had cookies implanted on their machines unless they took affirmative steps to reject cookies – the well-known "Opt-Out" scheme. It became additional work for the users as they had to have two menu screens down in his/her browser to find the place to opt out of cookies. There seemed to be no anticipation at the time that the use of cookies would create a problem!!

Security policy is a codified set of processes and procedures applied to secure the fulfillment of its obligations and the continuation of its activities even in the presence of possible interferences. A security policy can be an organizational policy, an issue-specific policy or a system-specific policy. Most companies also have policies for acceptable use of the Internet. Given the nature of security threats today, such a policy is necessary but not sufficient on its own. Its effective implementation draws from the continuous training to educate users about security policies. There is no doubt that without the technical means to enforce company policies, companies are at greater risk. Inconsistent enforcement of policies and making security rules on the fly makes disciplinary action harder. An effective web filtering and monitoring service can help enforce an Acceptable Usage Policy. A good system allows a high level of control over what types of sites can be blocked and helps maintain an extensive database of websites to make sure nothing falls through the cracks. Acceptable use of the Internet is addressed in Section 9.8.

Box 9.4 Cookies and Fair Information Practices to Avoid Privacy Loss

The Information Privacy Act of 1988 recognizes that it is often necessary to find a balance between the privacy interests of the person whose information is collected or handled and the legitimate interests of good government and other people. The 11 IPPs (Information Privacy Principles) set out general rules for organizations to apply – they are listed below to build the context for use of cookies with regard to "privacy."

Box 9.4 Cookies and Fair Information . . . (Continued)

1. **IPP1 – Collection:** Manner and purpose of collection of PI.
2. **IPP2 – Use and disclosure:** Solicitation of PI from individual concerned.
3. **IPP3 – Data quality:** Solicitation of PI generally.
4. **IPP4 – Data security:** Storage and security of PI.
5. **IPP5 – Openness:** Information relating to records kept by record-keeper.
6. **IPP6 – Access and correction:** Access to records containing PI.
7. **IPP7 – Identifiers:** Alteration of records containing PI.
8. **IPP8 – Anonymity:** Record-keeper to check accuracy, etc., of PI before use.
9. **IPP9 – Transborder data flows:** PI to be used only for relevant purposes.
10. **IPP10 – Sensitive information:** Limits on use of PI.
11. **IPP11 – Limited disclosure:** Limits on the disclosure of PI.

Many cybercrimes take place by stealing people's PI (ID theft, Phishing, etc.). People's private information stolen can be used for cybercrimes. Privacy mature organizations understand this and they protect privacy of their employees, prospective employees, customers and prospective customers as well as associates (contractors, consultants, trainers, etc.). There are a number of "Privacy Best Practices" around the cookies:

1. According to the "Openness Principle" users/Internet site visitors need to be informed of all data collection, including implicit collection such as cookies, behavioral tracking, etc.
2. Avoid storing PII in cookies if it is necessary to store PII in cookies then encrypt it.
3. Do not store cookies for longer than they are needed. Use session cookies whenever possible.
4. Limit scope of cookies whenever possible. Limit it to application, directory or host.
5. On your company website, the privacy policy needs to be clearly displayed and disclose when and why cookies are used.
6. When possible, make site accessible without cookies for users who turn them off or delete them – provide persistent Opt-Out cookie mechanism, especially for third-party cookies.
7. Avoid cookie-like mechanisms that are difficult for users to control (e.g., flash cookies that are local-shared objects).

As mentioned earlier, the topic of cookies is controversial and one cannot make a general statement that cookies are always bad. Cookies themselves are not inherently bad or necessarily invasive to one's privacy. They are instrumental in activating some of the Web's most appealing features. You must have noticed that when you browse amazon.com you get many suggestions about books on the topic that you are looking for. How do you think that happens? Merchants like Amazon.com use cookies to speed ordering and to suggest products to customers. Search results would be slow without cookies. It is the rising number of third-party advertising networks that made the topic of cookies controversial and raised the issue of cookies to prominence in legal and policy-making circles.

Monitoring and Controlling Employees' Internet Surfing



A powerful deterrent can be created through effective monitoring and reporting of employees' Internet surfing.

Even organizations with restrictive policies can justify a degree of relaxation; for example, allowing employees to access personal sites only during the lunch hour or during specified hours. However, without such effective reports, organizations are just blind. With appropriate use of tools, managers get insight into employees' web use. Considering the close association of "cookies" with websites visited during Internet surfing,

HR investigations become possible, thus giving managers a broad picture of company-wide usage patterns and productivity.

Keeping Security Patches and Virus Signatures Up to Date

Updating security patches and virus signatures have now become a reality of life, a necessary activity for safety in the cyberworld! Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management. Doing it properly and regularly absorbs a significant amount of time. At the same time, not doing it properly exposes IT systems to unnecessary risk. Typically in-house web filters, policy engines, Spam and anti-malware systems need regular updates to stay effective. Finding IT technicians with the right level of skill to manage these systems is another aspect of this problem. For the IT resources such mundane activities become boring as they do not see it adding any value to their resumes.

Box 9.5

Organizations Have the Choice: Proactive vs. Reactive Approach to Security

Proactive approaches are the measures taken with the aim to thwart host-based or network-based attacks from successfully compromising systems. On the other hand, reactive approaches are the procedures used after it has been discovered that some of organization's systems have been compromised by an intruder or attack program. Resources ought to be dedicated to the prevention of expensive damages that may occur if such preventive measures are not taken. For example, banks use thick steel and concrete vaults with advanced electronic systems to prevent and detect break-ins. Many organizations use cameras to record business activities. In doing this, the idea is that cameras both deter theft and help identify perpetrators when thefts do occur. Some organizations use Intrusion Detection and Response Systems (IDRSes) in an attempt to detect computer intrusions and then activate defensive measures when an attack is detected. All these are examples of proactive approaches to secure an organization's infrastructure.

Proactive measures help prevent future business losses; however, organizations also need to respond to such losses when the proactive measures either were not either effective or did not exist. This is where reactive approach comes into picture. Reactive methods include Disaster Recovery Plans (DRPs – for more information about disaster recovery plans and business continuity planning, see Ref. #9, Books, Further Reading), use of forensics investigation and loss recovery specialists, reinstallation of OS and applications on compromised systems, or switching to alternate systems in other locations (hot sites and warm sites). Preparing an appropriate set of reactive responses and being ready to implement is just as important as having proactive measures in place. In reality, it is not easy to decide the distribution of resources (time, money, people) for proactive measures vis-à-vis that for reactive measures. These decisions can be further complicated by the choice available, that is, whether to use in-house resources or to outsource.

The 2009 survey of Data Security Council of India (DSCI) revealed the state of data security in the Indian industry. The five "most implemented tools" by Indian industries, turned out to be:

1. Antivirus/anti-Spyware installed at the endpoints.
2. Antivirus (messaging systems).
3. User ID/password protection.
4. Anti-Spam.
5. Patch management.

You can refer to this report: http://www.naavi.org/cl_editorial_10/data_security_survey_2009_report_final_30th_dec_2009.pdf (30 September 2010). A detailed discussion about operating system security and importance of patch management is available in Ref. #10, Books, Further Reading.

Surviving in the Era of Legal Risks

As website galore, most organizations get worried about employees visiting inappropriate or offensive websites. We mentioned about Children's Online Privacy Protection Act (COPPA) in Chapter 1. For example, if employees download images involving child pornography, or if they download pirated software, then directors can personally be held liable. Similarly, downloading other inappropriate images result in a hostile environment for coworkers. Poorly judged or irresponsible comments made by employees on public Internet forums can be slanderous or breach of confidentiality guidelines. It is quite challenging to address these legal risks. However, organizations with effective web filtering and monitoring can provide reassurance and reduce risks. The topic of "privacy threats to organization due to social media marketing" is addressed in Section 9.5.



Serious legal liabilities arise for businesses from employee's misuse/inappropriate use of the Internet.

Bandwidth Wastage Issues

Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images. At the same time, there is a considerable rise in workforce mobility and many remote connections to work networks are through the virtual private network (VPN). Organizations have to pay for their bandwidth utilization. Under such a scenario, there is a concern when expensive bandwidth is wasted by non-work Internet use. With the rise of social networking and the trend toward social media marketing (addressed in Section 9.5), streaming audio and video sites and TV-on-demand business, Internet connections are under severe strain. A considerable percentage of a business's bandwidth gets used for non-work Internet access. This indeed is a waste of money and it reduces the bandwidth available for legitimate work. The result is slower E-Mail, slower web browsing and slower VPN connections.



There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

Using sophisticated policy controls, you can get such tools to block banned websites, downloads, E-Mail Spam and media streams your own systems before they reach your network. This helps increase work productivity by preserving the bandwidth for real work. You can also use the tools to protect remote working employees as well as employees working from home. It can preserve expensive wireless broadband connections and homeworker's links back to the company network.

Mobile Workers Pose Security Challenges

Use of mobile handset devices in cybercrimes is discussed in Chapter 3. Most mobile communication devices – for example, the personal digital assistant (PDAs) and RIM BlackBerries – have raised security concerns associated with their use (The Indian Express review on 13 August 2010, p. 16). Mobile workers use those devices to connect with their company networks when they are on the move. Even if organizations have in-house systems to monitor and control web access and to protect web users from malware, those systems often may not be capable of covering remote users working on laptops and homeworkers

operating outside the corporate firewall. This means that there is a significant part of the workforce that remains unprotected. Most organizations see this as a serious issue that can threaten organizational security. You need tools that extend web protection and filtering to remote users, including policy enforcement. Such tools can ensure remote users' online activities that are tracked by the tool's reporting mechanisms.

Challenges in Controlling Access to Web Applications

Today, a large number of organizations' applications are web based. There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications; now cloud computing too is added to that repertoire. Employees often tend to use these applications to bypass corporate guidelines on security; for example, to access personal E-Mail or upload company data to services outside company control. At times, employees may use their personal E-Mail IDs to send business-sensitive information (BSI) for valid or otherwise reasons. For example, an employee was unable to use his/her company mail application or perhaps was unable to access the mail server of the company when sending information that was urgent in business context. Instances such as these reduce IT department's control over data and security. More and more organizations are getting worried about employee access to webmail or instant messaging applications. As the sophistication of online applications increases, this is going to become a significant problem.

Thus, organizations need to decide what type of access they should provide to employees. Some organizations will want to block non-work sites completely whereas others will want to allow access to some sites or within certain time limits. Given the nature of working style these days, organizations will allow employees access to approved online services, such as hosted customer relationship management (CRM) applications. You can select tools that provide granular control over which sites are allowed and which are banned from being accessed. It is possible to limit access to personal sites during office hours with time limits.

The Bane of Malware



Malware, viruses and Trojans are discussed in Chapter 2.

Their consequences are explained in Section 9.2.1 with regard to costs involved when organizations are impacted by cyberattacks. Many websites contain malware. Such websites are a growing security threat. Although most organizations are doing a good job of blocking sites declared dangerous, cyberattackers, too, are learning. Criminals change their techniques rapidly to avoid detection. The consequences of infection are severe compared with any kind of malware. It saps organization's energy because virus clean-up takes time, diverts IT resources and costs money. Infection makes company's confidential information vulnerable and undermines the IT department's efforts to provide assurance to the board about security. There is a point of caution with anti-malware tools – some organizations may develop a false sense of security about their protection. Only website-based malware is evolving rapidly and is growing in technical sophistication. Due to this, it becomes essential to have protection that goes beyond signature detection. There are tools and services that offer a combination of signature scanning and advanced heuristic protection using proprietary technology.

It looks like producing malware and Malicious Codes have become an industry within the organized criminal syndicates. In such a milieu, security risks and dangers faced by users of pirated software are only rising day by day. Organizations that ignore the issue of pirated software could be exposing themselves to security risks, with implications such as loss of data, confidentiality, and integrity and reduced operational

performance. With today's networked environment with computing devices connected through the Internet, such threats arising from infected non-genuine software have far reaching implications for an entire network.

The Need for Protecting Multiple Offices and Locations

Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today. Most large organizations have several offices at multiple locations. Protecting information security and data privacy at multiple sites is indeed a major issue primarily because protecting a single site itself is a challenge these days. In a solo site scenario, you need anti-malware, web filtering and monitoring software and all the support needed to keep it up to date. Additional effort is required with multiple sites, as all hardware and administrative overheads are multiplied! In such a scenario, an Internet-based-hosted service that can easily protect many offices is worth considering. For an Internet-based-hosted service, it does not matter how many E-Mail servers there are. However, with in-house solutions, you do not have to pay an upfront capital cost for hardware and software followed by an unpredictable ongoing maintenance cost. Fixed fee per user is also an option to consider.

9.4 Security and Privacy Implications from Cloud Computing

A report available at the link <http://www.aakashjain.com/misc/10-cyber-threats-to-look-for-in-2009-648> (8 October 2010) indicates that cloud computing is one of the top 10 cyberthreats to organizations. Recall the discussion in Chapter 2 (Section 2.8) about cloud computing. There are some piquant issues that come with cloud computing. For example, think about this – if at all you entrust a cloud provider with your data, how will the vendor handle data encryption? What about user authentication? Who will own the liability in case of data breach? There are data privacy risks associated with cloud computing. Basically, putting data in the cloud may impact privacy rights, obligations and status. There is much legal uncertainty about privacy rights in the cloud. Organizations should think about the privacy scenarios in terms of "user spheres." There are three kinds of spheres and their characteristics are as follows:

1. **User sphere:** Here data is stored on users' desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to users and monitor that access to ensure misuse does not happen. The challenges to consider are: What data is transferred from the client to a data recipient? Is the user explicitly involved in the transfer? Is the user aware of remote and/or local application storing data on his system? Is data storage transient or persistent?
2. **Recipient sphere:** Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data. In this sphere, organization's responsibility is to minimize users' privacy risks by ensuring that unwanted exposures of personal data of users do not happen. The challenges to consider are: What data is being shared by the data recipient with other parties? Can the user expect or anticipate a transfer of his data by the recipient? Is personal data adequately secured? Is data storage transient or persistent? Can the processing of personal data be foreseen by the user? Are there any secondary uses of data that may not be foreseen by the user? Is there a way to minimize processing (e.g., by delegating some preprocessing to user sphere)?
3. **Joint sphere:** Here data lies with web service provider's servers and databases. This is the in-between sphere where it is not clear to whom does the data belong: to the users (data owners/data senders) or to data recipient. Cloud computing has this scenario. Here organization's responsibility is to provide

to users some control over access to themselves (in terms of access to data and attention) and to minimize users' future privacy risks. The challenge to handle is: Is the user fully aware of how his/her data is used and can he/she control this?

9.5 Social Media Marketing: Security Risks and Perils for Organizations



Of late, social media marketing has become dominant in the industry.

Social computing (addressed in Section 9.6) and social media marketing cannot be separated. Social media is rapidly growing in importance. Gartner Inc. predicts that around 20% of business users will be using the so-called social networking services as their most important communication tools by 2014! According to fall 2009 survey by marketing professionals, usage of social media sites by large business-to-business (B2B) organizations shows the following:

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. MySpace is used by 6% of the organizations.

Data breach offenses and data stealing incidents are rampant in most other countries. Cybercriminals are on lookout for exploiting information to their advantage. The Internet has penetrated India in a big way and due to this security breach incidences are on the rise. Hackers use a number of Internet channels such as the Web, E-Mail, instant messaging, Voice over Internet Protocol (VoIP), etc. to launch sophisticated and targeted attack to steal information from which they can benefit financially. Although "Phishing" (refer to Chapters 2 and 5) is a major threat for organizations, it is not the only one. Organizations today face one more threat – almost three quarters of malicious content is now contained in legitimate sites! It is worth noting that security attacks are becoming data-centric. Although the euphoria about social media marketing practice is high (seems mainly due to competitive pressures), organizations must protect their data.



Although the use of social media marketing site is rampant, there is a problem related to "social computing" or "social media marketing" – the problem of privacy threats.

Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of "social media marketing." The phenomenon called "social media marketing" and the reasons why it is used is worth understanding.

There are professional networks/social media sites such as the LinkedIn and many others such as Facebook, Orkut, MySpace, etc. (refer to discussion in Chapter 7, Section 7.14). In simple words, "social media marketing" is an approach that makes use of social media sites to enhance the visibility on the Internet so as to promote products and services. People find that social media sites are useful for building social (and business) networks and for exchanging ideas and knowledge. Figure 9.8 shows different types of social media tools.

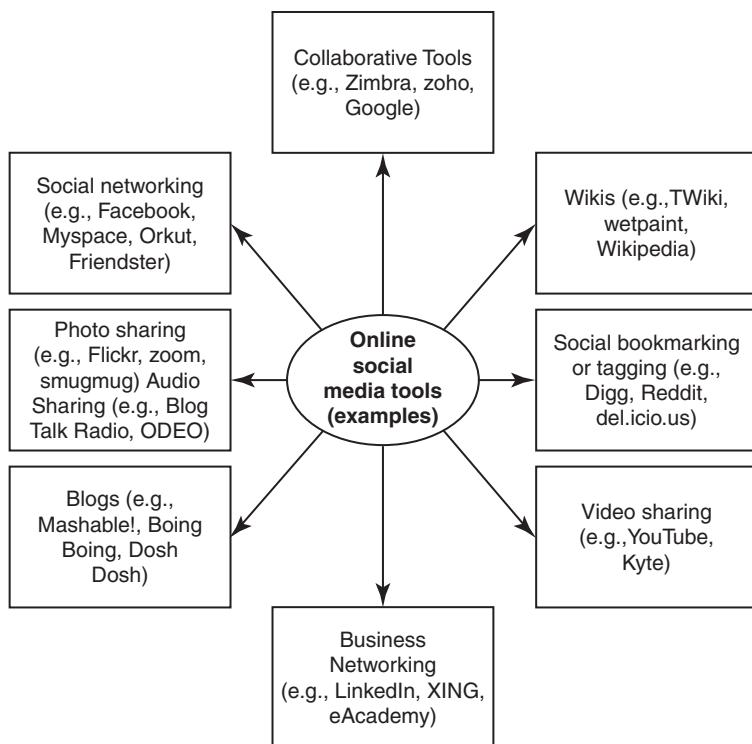


Figure 9.8 | Social media – online tools.

9.5.1 Understanding Social Media Marketing

Most professionals today use social technologies for business purposes. Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development, etc. There is no doubt that the boost to social media marketing has happened due to phenomenal growth of the Internet. The Net has become an integral part of our life. We attend meetings, dinner parties and sales meeting parties or even dealer meets, etc. where we have social interactions amongst people and we discuss our experience of a brand that we like! Social media marketing uses a number of tools to reach out to larger audience; for example podcasts, wikis, blogs, folksonomies, online videos, photo sharing, news sharing, message boards and posts on social networking sites. Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
2. To increase traffic to their website coming from other social media websites by using Blogs and social and business-networking. Companies believe that this, in turn, may increase their “page rank” resulting in increased traffic from leading search engines.
3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.

4. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
5. To collect potential customer profiles. Social media sites have information such as user profile data, which can be used to target a specific set of users for advertising (recall the discussion about "cookies" in Box 9.2).

In addition to the social media online tools mentioned in Fig. 9.8, there are other tools too that organizations use; industry practices indicate the following:

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
2. Professional networking tool LinkedIn is used to connect with and create a community of top executives from the Fortune 500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
4. YouTube (the video capability tool to run demonstrations of products/services, etc.) is used to increase the brand awareness and create a presence for corporate videos.
5. Wikipedia is also used for brand building and driving traffic.

Thus, we can see that popular social media sites are becoming very popular these days. By definition, social media websites are more open than traditional sites. As the Web continues to grow and evolve with the adoption of Web 2.0 applications, virus outbreaks and other forms of web-borne threats known as "malware" continue to grow as well. Links of useful information on Web 2.0 are provided in Ref. #22, Additional Useful Web References, Further Reading. This is how security risk comes into picture when using social media online tools depicted in Fig. 9.8. As such, users must ensure that they have adequate web security to protect them against Web 2.0 threats. It is good to use multi-layered solutions that have an array of analysis techniques (e.g., antivirus signatures and network intelligence heuristics, behavioral analysis, etc. that may help real-time analysis of URLs) including real-time scanning. There are many web security solution vendor companies that offer specialized solutions that can be located on the Internet. However, that discussion is not within the scope of this chapter – we have provided a useful link in Ref. #11, Additional Useful Web References, Further Reading.

There are conflicting views in organizations about use of social media marketing. Some people in the IT industry express concerns about the excessive and careless use of social marketing media given the security threats associated with them, whereas some say that the benefits from social media marketing (described previously in this section) outweigh the security risks. Some organizations ban the use of social networks. Such security concerns limit the high potential that social media offers for marketing, sales and corporate communication.

9.5.2 Best Practices with Use of Social Media Marketing Tools

First and foremost, it is essential to establish a "social media policy." Use of personal blogging for work-related matters should be monitored and minimized. Recall the discussion in Section 9.3.1 "Employee Time Wasted on Internet Surfing" about employees endlessly surfing on the Internet during the work hours. Use of policies and implementation of policy-based procedures are always essential – Section 9.3.1 addressed "Enforcing Policy Usage in the Organization". Once the policy is created, employers should communicate it to employees and should enforce its implementation through continuous monitoring.

Increasing employee awareness is an ongoing activity. There is no go without it. This is because people can change their way of behaving in social networks only if they are aware of the security risks; sometimes

they are genuinely not aware of those risks. Therefore, organizations need to educate their employees about the risks associated with the use of online social media tool. Organizations must raise their employees' awareness of the fact that even seemingly innocuous information can reveal too much about the company or the person's private life. Providing continuous information about new security threats and maintaining rules of conduct can enhance employee awareness. On the basis of staffing budget available in the organization, it is worth exploring appointment of a social media expert within the company. Such an expert can serve as a permanent contact for employees for their questions on social media marketing tool usage especially when the staff is engaged in marketing activities.

Once you have social media usage policy in place, next steps are to establish firm processes based on that policy. Network security administrators need to remain up to date about the most recent risks on the Web. There is a strong need to establish firm processes that are systematically linked to daily workflows. Such processes should be easy to implement and audit. For example, administrators should ensure that the latest security updates are downloaded. Although it seems to be mundane and boring activity, it is crucial. Organizations must enable their IT administrators to identify network attacks in time or to avoid them altogether. IDS and firewalls play a crucial role here. Refer to Ref. #2, Books, Further Reading for a detail discussion on IDS and firewalls.

Mere policies and procedures are of no use if you do not have the mechanism to maintain a strong controls posture. With organization guidelines available, network administrators find it easier to define the network domain as well as the applications that can be accessed by specific people at specific times. For this, you need to establish the "need-based access policy." Once you have this in place, it becomes possible to control and monitor access to critical data, and to track such access at any time. Doing this reduces the risk of information falling into wrong hands through unauthorized channels. Thus, strong access control policies and monitoring of user accesses in an ongoing manner is essential. Compliance requirements should also be taken into consideration. Policies should not be treated as a one-time activity. The important thing is to keep the policies up to date and adapt them to changing circumstances. Access management is addressed in Section 9.11.

Blocking the infected websites is another necessary activity. Recall the discussion about Trojan, viruses, worms, etc. in Chapter 2 – an action such as a person clicking on an infected website to download a Trojan can happen even when employees are taken through regular awareness training. Attrition in the organizations means that well-aware employees leave and new employees join! URL filters allow organizations to block access to known malware and Phishing websites (Phishing is discussed in Chapter 5). Access blocking can also be applied to any other suspicious site on the Internet. The filter function should be kept continuously up to date by maintaining so-called black- and white-listed websites.

Firewalls help to protect the organization (for more information refer to Ref. #2, Books, Further Reading). Using next-generation firewalls helps organizations keep their security technology up to date. Some firewalls provide a comprehensive analysis of all data traffic. Deep inspection of network traffic makes it possible to monitor the type of data traffic, the websites from which it is coming, to know the web browsing patterns and peer-to-peer applications to encrypted data traffic in SSL tunnel. (For Secure Socket Layer – SSL refer to Ref. #3, Books, Further Reading.) SSL is a process for inspection. The firewall decrypts the SSL data stream for inspection and encrypts it again before forwarding the data to the network. This results in effective protection of workstations and other endpoints, internal networks, hosts and servers against attacks within SSL tunnels.

Protection against vulnerability is possible by carefully planning vulnerability scanning and penetration testing (refer to Ref. #6, Books, Further Reading). Vulnerabilities present a huge challenge to any corporate network. In addition to the routine risks, organizations need to worry about the fact that attacks on vulnerabilities via the social web services are steadily increasing. An intrusion prevention system (IPS) serves as a protective barrier to the corporate network. An IPS automatically prevents attacks by worms, viruses or other

malware (refer to discussion in Chapter 2). Having identified an attack, the IPS immediately stops it and prevents it from spreading in the network. The IPS also enables patching of servers and services by securing servers under security threat, which will then be patched during the next maintenance window.

We mentioned about “need-based” access; organizations should define access to business applications that reside on corporate networks as well on the external sites. In Chapter 3, there is a discussion about careless use of mobile devices contributing to cybercrimes. There is a phenomenal rise in workforce mobility; mobile users, partners and distributors often need to access a corporate network while away from work place. Within this group, the use of social media can be monitored only on a very limited basis or not at all. This makes it even more important to assign the rights for defining all network access centrally, for example, using an SSL VPN portal – VPN is virtual private network, a tunnel within the Internet. At the same time, on the user level a strong authentication via single sign-on makes the administrator’s work easier. As a result, a single login makes it possible for users to access only the network areas and services for which they are authorized. Readers can refer to presentation and subsequent article on workforce mobility and challenges.^[1]

Even the Intranets are not spared by cyberattackers. Therefore, securing the Intranets should also be included in the protection activities. The Intranet of every company contains highly sensitive information pertaining to the business areas involved (see Table 9.1). These areas need to be isolated from the rest of the

Table 9.1 | Business area-wise information

<i>Business Area</i>	<i>Coverage</i>	<i>Typical Examples</i>	<i>Remarks</i>
Business environment	Business conditions external to the organization that can impact its business activities	<ul style="list-style-type: none"> 1. Rules and compliance set by regulatory agencies 2. Issues created by Competitors 3. Licensing authorities’ requirements 	These may not be handled in a computerized manner inside a company data warehouse
Customers and other affinity organizations	People and organizations who acquire and/or use the company’s products	<ul style="list-style-type: none"> 1. Prospects 2. Customers 	Organizations use these mechanisms for capturing potential customers (prospects) and for distinguishing between parties who buy the product and those who use it
Communications	Messages and the media used to transmit them	<ul style="list-style-type: none"> 1. Advertisement campaigns 2. Target audience 3. Company websites 	These often pertain to marketing/prospecting activities. They can also apply to internal and other communications
External organizations	Organizations, except customers and suppliers, external to the company	<ul style="list-style-type: none"> 1. Complementors/business partners 2. Existing competitors 3. Potential competitors 	In the paradigm of “networked organizations” of today, this inclusion is important
Facilities and equipments	Real estate and structures and their related components, movable machinery, devices, tools and their integrated components	<ul style="list-style-type: none"> 1. Buildings and surroundings 2. Heavy machinery 3. Testing and other equipments 4. Factories 	Software that is integral to equipments is included within this area; other software is included within information area. Integrated components (e.g., security alarm system within an office or plant) are often included as a part of the facility

internal network by using the firewalls to segment the Intranet. This enables segregation of departmental Intranets; for example, a company can separate departments such as finance or accounting from the rest of the Intranet and thereby prevent infections from penetrating these critical segments of the corporate network. Figure 9.9 shows the diagram of the firewall with two demilitarized zone (DMZ) networks.

If there is a need to use an existing multiple network segments then you can deploy multiple DMZ with differing security policies (levels). For example, you may need to deploy the applications for Extranets, Intranets, web server hosting and remote access gateways (see Fig. 9.9).



In Chapter 3, it is explained how the unmonitored and careless use of mobile handset devices can contribute to loss of cybersecurity and how cybercrimes can be committed using mobile devices.

Given the small size of mobile devices coupled with their phenomenal features, they cannot be ignored. Therefore, it is a good idea to include mobile devices in the security policy. It is common for users to navigate social web services with mobile devices such as laptops, PDAs and Smartphones (refer to Chapter 3; Fig. 3.1) – the same devices are used by users to log into the corporate network. The corporate security department, therefore, needs to include mobile devices in the security policies. This can be done, for example, with the assessment function by checking the login device for the required security settings and for the presence of security-relevant software packages. Through this function, it can be checked whether the proper and latest host firewall is installed and whether both the OS and antivirus software as well as all patches are up to date.

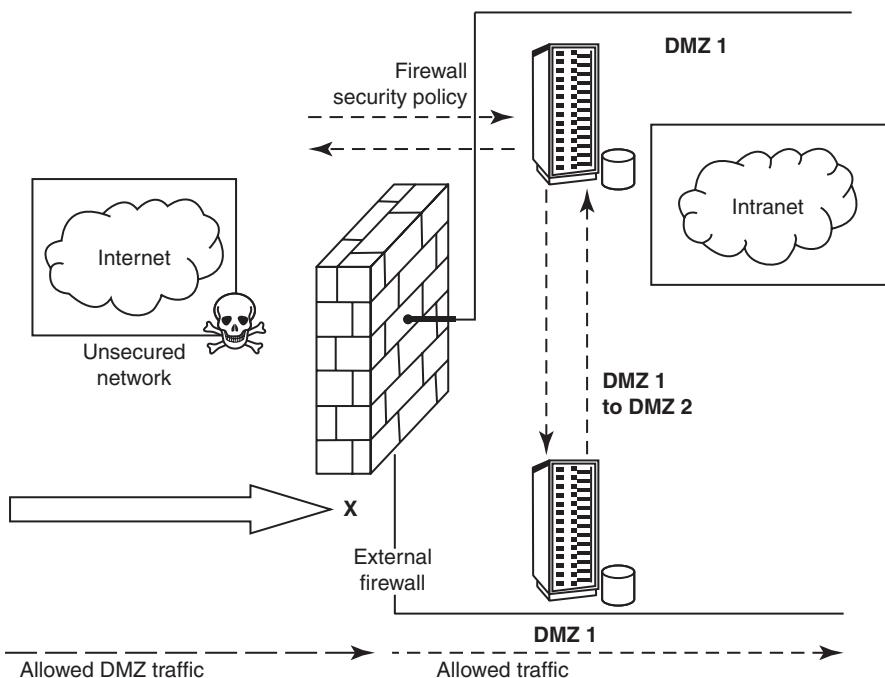


Figure 9.9 | Firewall with DMZ networks.

Even if one of these criteria is not met, automatically, access should be denied to the device or access may be provided only on a limited basis. On the basis of necessity warranted by a situation, mobile devices can be forwarded directly to a website containing the required updates.

With the use of centralized management, administrators can manage, monitor and configure the entire network and all devices using a single management console. They can also monitor user activities on the network by viewing reports. For example, system administrators will be able to know who has accessed which data at what time. This allows preventing attacks more effectively and provides more efficient protection for corporate applications at risk. A central management console also makes it possible to roll out and maintain standard security guidelines for the entire corporate network. Given these issues, risks and challenges involved with the use of social media marketing tools, indeed the involvement of the senior employees of the organization is critical to the success of the social media marketing initiative. Although organizations scurry to social media marketing techniques remain competitive and look “modern,” they should take due care to avoid loss of reputation. Organizations also ensure corporate compliance. To conclude this section, the organizational best practices are listed below:

1. Organization-wide information systems security policy;
2. configuration/change control and management;
3. risk assessment and management;
4. standardized software configurations that satisfy the information systems security policy;
5. security awareness and training;
6. contingency planning, continuity of operations and disaster recovery planning;
7. certification and accreditation (refer to Chapter 12 in CD).

9.6 Social Computing and the Associated Challenges for Organizations

Social computing is also known as “Web 2.0” – it empowers people to use Web-based public products and services. Social computing is much more than just individual networking and entertainment. It helps thousands of people across the globe to support their work, health, learning, getting entertained and citizenship tasks in a number of innovative ways. In the modern era, we are “constantly connected,” business is “24 × 7” – the business where world never sleeps. People carry anxieties in a competitive business world. In such a milieu, people and organizations are appreciating the “power of social media.” Business is taken forward based on how connections are made through social networks. In this process, a lot of information gets exchanged and some of that could be confidential, Personally Identifiable Information (PII)/SPI, etc. This would be a gold mine for the cybercriminals. “Social networking,” “social media marketing” (addressed in Section 9.5) and “social computing” are not unrelated concepts. There is a new genre of challenges, though they come with rising use of social computing and organizations need to watch for these challenges. For example, social computing poses the risk of “digital divide.” Getting too used to readily available information, people may get into the mode of not questioning the accuracy and reliability of information that they readily get on the Internet. With social computing, there are new threats emerging; those threats relate to security, safety and privacy. How to protect one’s online privacy is in fact a major preoccupation for people all over the world; particularly in European countries where there is a very high consciousness about privacy loss. Impersonation and identity theft are some of the new risks as discussed in Chapter 5. Cyberbullying (explained in Box 2.8 of Chapter 2) and “online grooming” are the new emerging threats for children in particular. Over and above this, unclear data ownership and lack of controls in users hand for guarding their data are resulting into privacy invasion risks (cloud computing risks are discussed in Section 9.4).

Box 9.6 Protecting Your Online Privacy – You may be “Fingered”!

The term “Dataveillance” was coined in 1988 by Australian privacy expert Clarke. It is about monitoring people not through their actions but through data trails about them. “Personal Dataveillance” involves monitoring of “identified individuals” and “Mass Dataveillance” is about monitoring of whole populations. We mentioned about cookies in Boxes 9.2–9.4 how cookies are exploited by cybercriminals.

There are bigger threats emerging now. There is a new type of method, *browser fingerprinting*, to track you online! It can identify you far more accurately than any cookie – and you may never even know it was there! The method inauspiciously pulls together data about your browser, such as plug-ins, system fonts and your OS. The data, by itself does not identify you. Together, however, they become a digital fingerprint. It is like putting together several pieces of information – each in itself may not seem to reveal anything but together it tells a story. For example, to describe a person, you just mention “brown hair” and it does not seem to identify anyone. However, add-in pieces of descriptions such as “6 feet, 2 inches tall,” “chipped left front tooth,” “size 10 shoes” and so on are enough to pull someone out of a crowd, even without their name, Social Security Number or any other of the usual identifiers.

You may wonder how and where all this began. Banks had browser fingerprinting developed for their use to prevent fraud. Now, however, one company, Scout Analytics, offers browser fingerprinting as a service to websites, and it collects not just browser data but also data about how you type – things like your typing speed and typing patterns! Therefore, now it works like a biometric signature – such as the identifiers, collected from the browser and the computer, can be gathered using JavaScript alone, making this form of tracking hard to block. Countering this new privacy threat is not going to be simple – at least not as simple as deleting cookies. The big question to ask is “Can sites legally use this fingerprinting?”

You can test your browser for unique identifiers without the risk: the Electronic Frontier Foundation, a privacy advocacy group, has set up an interesting online experiment at Panopticlick. eff.org. Panopticlick gathers little details about your browser and computer, mostly using Javascript.

In a way, social computing is related to social media marketing because business leaders in product development, marketing and sales view social computing as an integral part of the evolving enterprise channel strategy. The CIOs, however, see it as a source of many security and privacy risks. Recommendation is to take due care while using social computing as a channel strategy for communicating with internal or external stakeholders such as employees, customers and suppliers.

9.7 Protecting People’s Privacy in the Organization

The costs associated with cybercrimes are discussed in Section 9.2. A key point in that discussion is that people perceive their PI/SPI to be very sensitive. From privacy perspective, people would hate to be monitored in terms of what they are doing, where they are moving, etc. An interesting question is: Will it become possible for India to track its citizens? Tracking and monitoring people’s transactions on the Internet is a controversial issue. RFIDs have been successful to track objects, animals, birds and goods in shipment. However, from privacy perspective, “use of RFIDs to track humans” is a highly controversial area – more on that can be read in Ref. #4, Books, Further Reading. Human issues in privacy and security are most complex. When it comes to information security and protection of “privacy,” the human resource area is known to throw some of the most complex challenges. We mentioned “insider threats” in the introduction section of the chapter – human greed has caused many evils; data theft is one of them in cybersecurity context.

In the US, Social Security Number is a well-established system/mechanism for uniquely identifying all American citizens; however, similar thoughts are now emerging in India. The UID Project was started by Government of India and is running through an agency called Unique Identification Authority of India (UIDAI) based on the similar concept. The purpose is to create a “multipurpose national identity card or unique identification card (UID Card).” The stated purpose of this project is very noble, although it means that people’s unique identification will get into the hands of the government. It is believed that the UID Project, through creating Unique National IDs, will help address a number of maladies in the country: the rigged state elections, widespread embezzlement that affects subsidies and poverty alleviation programs. It is also supposed to address illegal immigration into India and terrorist threats. Although the Indian Government has issued IDs, they are fragmented by purpose and region in India. This leads to widespread bribery, denial of public services and loss of income – it particularly makes citizens poor. When the unique identity database comes into existence, the number of identity databases (voter ID, passports, ration cards, licenses, fishing permits, border area ID cards) currently existing in India are supposed to be linked to it.

9.8 Organizational Guidelines for Internet Usage, Safe Computing Guidelines and Computer Usage Policy



Identity theft is addressed in detail in Chapter 5 – it is one of the biggest threats to individuals in today's era.

IT managers need to recognize the need for proactively protecting their company's identity when online. Each time an employee accesses the Internet, the individual may leak pieces of information to watchful competitors, hackers and online predators. Anonymizer effectively mitigates these threats with their identity protection and information assurance solutions; however, there are risks too associated with “Anonymizers” (see Box 9.7).

Box 9.7 Anonymizers: The Boon and the Bane!

Recall the discussion in Chapter 4 (Section 4.2) about “anonymizers.” There are many privacy-enhancing tools and technologies available today. Anonymizer is one such tool. Anonymizer websites act as agents on your behalf when you browse websites. Users log onto a website and type in a destination and the proxy server surfs the Web for them. The anonymizer then passes the results of the search back to their browser, often via an encrypted communications channel, to mask both the identity of the target website and the relayed contents. Thus, an “anonymizer” is a tool or proxy that hides a source computer's identifying information, protecting the end-users identity. Anonymizers are available for web surfing, E-Mail, instant messaging, etc. An example of anonymity by web proxy works is shown in Fig. 9.10. The web proxy acts as a proxy for users and hides information from end servers.

Internet anonymizers are, thus, services that make your web browsing as anonymous as possible. Anonymizer sites access the Internet on user's behalf and that way it protects your PI from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you and thereby it puts you away from the sites you visit, that is, it is the anonymizer that accesses the site on your behalf thus keeping your identity unexposed. There are anonymizer solutions available to circumvent security threats by completely masking the network identity while users are online. This is achieved by combining a series of techniques such as secure high-performance network access, the use of variable IP addresses and the application of preregistered domain names. These features make it statistically impossible for any organization to trace back and uncover their true corporate identity.

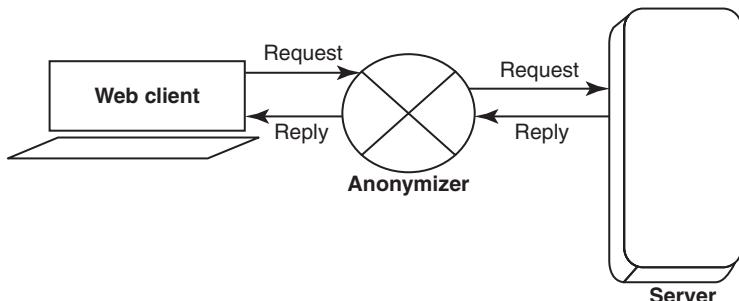
Box 9.7 Anonymizers . . . (Continued)


Figure 9.10 | Anonymity by web proxy.

We must understand that anonymizers may not guarantee 100% privacy because they are not entirely secure. An anonymizer keeps logs of incoming and outgoing connections and if it is physically located in a country where it is subjected to warrant searches then there is a potential risk that government officials can trace to identify all users who used the anonymizer and how they used it. Although most anonymizers claim that they do not keep logs, currently there is no method for confirming that. However, if the user used another anonymizer to connect to the exposed anonymizer then that user is still anonymous.

In Section 9.3.1, it was mentioned that uncontrolled use of web creates a nuisance for organizations by hogging the network bandwidth for downloading large audio and video files, and encouraging time wasters to engage in non-work-related web surfing. Uncontrolled web use carries significant risks. In schools and libraries, anonymizers are the most popular tool students use to access top social web destinations such as YouTube, MySpace and Facebook, typically blocked by school IT staffs. Anonymizers also circumvent blocks to potentially harmful sites prohibited by Acceptable Usage Policy. Even innocuous social websites can be frequented by sexual predators or serve as a launch pad for harassment. Cyberbullying incidents range from 18% to 42% of students in grades 4 through 8. In addition, small children get bullied online. Anonymizers create huge network security holes, hacker portals for data theft, Spyware, viruses and worms – users are completely unaware of their dangers. Anonymizer sites and fringe sites that offer illegal or offensive content often covertly deliver malware applications. For example, even after the original computer user logs off, the machine can start delivering offensive pop-ups to other users who log on to that computer.

Read the article “Are proxy Anonymizers putting Your enterprise in Peril? at: http://www.8e6.com/documents/pdfs/white_papers/2008_Are_Proxy_Anonymizers_Putting_Your_Enterprise_in_Peril.pdf (1 October 2010). List of websites for free proxy servers are quoted at the end of Section 4.2 in Chapter 4.

In view of the cyberthreats, it becomes cardinally important for organizations to develop *Safe Computing Guideline*. They are sometimes referred to as *Organizational Guidelines for the Internet Usage or Computer Usage Policy*. This is the topic of focus in this section as emphasized in Section 9.3.1 “Employee Time Wasted on Internet Surfing.” Policies are always important as they provide an objective and direction for implementation. Therefore, first we will start with *computer usage policy*. In the discussion that follows, an example of a public library is provided to explain each element in the policy. These are examples only and these are not the only way to describe the policy.

9.8.1 Developing an Organizational Policy for Computer Usage

At the basic level, a “computer usage policy” should address the following elements.

Mission Statement

First, the policy should briefly but meaningfully state the organization’s “mission” because policies must support the mission of the organization.

Public Library Example

Assuming that the library makes provisions for access to the Internet, the mission statement could read like:

“<XYZ> Library system provides the public of so and so area <ABC> with excellent service and convenient access to resources for their educational, informational, and recreational needs.”

Introduction

This section should explain what the policy document is about and what it contains as well as the scope of the policy.

Public Library Example

“This is a policy document and it constitutes a library-wide policy for the management of computer data networks and the resources they make available, as well as stand-alone computers that are owned and administered by the library. The policy supports the ethical principles of the library and indicates, in general, what privileges and responsibilities are characteristic of the library computing environment.”

Internet Safety

This is a very important section of the policy document

Public Library Example

“<XYZ> Library addresses the following Internet safety issues through its Acceptable Use Agreement, Parental Permission Form, and the use of technology protection measures on library computers.” The policy could further address the following elements:

1. Access by minors to inappropriate matter on the Internet and world wide web.
2. The safety and security of minors during usage of E-Mail, chat rooms and other forms of direct electronic communications.
3. Unauthorized access, including “hacking” and other unlawful activities by minors online.
4. Unauthorized disclosure, use and dissemination of personal identification information regarding minors.
5. Measures designed to restrict minors’ access to materials harmful to minors.

Next, subsection in this Internet safety should address the technology protection measure.

Public Library Example

“The term ‘technology protection measure’ means a specific technology that blocks or filters Internet access to visual depictions that are considered inappropriate for our patrons.”

Next, there should be a mention about the policy on use of *wireless Internet access*.

Public Library Example

"We provide unfiltered wireless Internet access to patrons who have their own hardware and software complying with the prevailing local regulations about activities that are not considered harmful with Internet usage."

Confidentiality

This constitutes a very important section in a policy about safe computing.

Public Library Example

"The Library shall treat data stored on computers as confidential (whether or not that information is protected by the computer operating system)." Considering that it is a public library, in this section a warning can be mentioned as shown below.

There can also be a mention about the conditions under which disclosure of information would be honored. As mentioned above it is a good idea to provide a warning about use of E-Mail facility.

Public Library Example

"Warning: Patrons, who use E-Mail systems, should be aware that E-Mail in its present form cannot be secured and is, therefore, extremely vulnerable to unauthorized access and modification."

User Responsibilities

This constitutes another very important section in a policy about safe computing.

Public Library Example

1. Users must sign an "Acceptable Use Agreement" or an Application for Borrower's Card to use full access to Internet stations.
2. Users granted with full access to Internet stations, must use either their own valid library card or their own valid guest card issued by the library. Photo identification shall be used to verify the identity of a registered patron if necessary. To obtain a photo ID card, please refer to the circulation policy of this library.
3. The library cannot control the content of material accessible electronically; therefore, individual users must accept responsibility for information accessed.
4. Users are responsible for payment of printing fees incurred.
5. Users should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these processes.
6. Computer accounts, passwords, library cards or guest cards and other types of authorization that are assigned to individual users are NOT transferable; they must NOT be shared with others.
7. Ultimate responsibility for resolution of problems related to the invasion of the user's privacy or loss of data rests with the user. The library assumes no liability for loss or damage to the user's data or for any damage or any other loss arising from invasion of the user's privacy.



Children's online safety is important. Refer to Chapters 1 and 6 where COPPA is mentioned.

Refer to Chapter 1 (Section 1.5.13) about pornographic offenses and COPPA and Chapter 6 about online safety and cybercrime laws (Section 6.2.2). These aspects are important to take into consideration while drafting a policy for safe computing. The prevailing laws must be consulted while doing that.

Public Library Example

"Minor children (under 18 years of age) are expected to be under the supervision of their parents or legal guardians who are encouraged to provide guidance to their own children. Parents or legal guardians are solely responsible for their child's/wards, use of the Library's electronic resources. Parents and legal guardians must grant permission for their minor children/wards to use the Internet by signing the Library Application for Borrower's Card or the Acceptable Use Agreement."

"Legal responsibilities" is an important aspect to be underlined in the user responsibilities section of the safe computing policy. Often the Internet access gets misused, leading to the onslaught of cyberattacks and the resultant damage to organizations as discussed in Section 9.2. Relate the public library example below to the discussion in Chapter 1 (Section 1.5.13) about "Offenses."

Public Library Example

Use by public and staff is restricted only to availing computing resources and that too for legal purposes only. Examples of unacceptable purposes include, but are not limited to, the following:

1. Harassment of others;
2. libeling or slandering others;
3. destruction of or damage to equipment, software or data belonging to the library or others;
4. disruption or unauthorized monitoring of electronic communications;
5. unauthorized copying of copyright-protected material;
6. using any computer for illegal or criminal purposes;
7. using any computer as a staging ground to "crack" or "hack" any computer system.

It is not only the "legal use" that is important but "ethical use" of computing policies is also important though it may not be addressed in any "security" standard. Therefore, a complete safe computing policy must address the ethical use also.

Public Library Example

Patrons are expected to use computing resources in accordance with the ethical standards of the library. Following are few examples of unacceptable use – note that some of these uses may also have legal consequences:

1. Unauthorized use of computer accounts or access codes.
2. Violation of computer system security.
3. Use of computer communications facilitates in ways that unnecessarily impede the computing activities of others (such as randomly initiating interactive electronic communications or E-Mail exchanges, overuse of interactive network utilities, etc.).
4. Software license agreements violation.
5. Violation of network usage policies and regulations.
6. Violating another user's privacy.
7. Making disruptive use of computers that could be detrimental to library service.



Just as user responsibilities are addressed, organizational responsibilities should also be addressed in a safe computing policy because both are important entities in safe computing.

Public Library Example

On the basis of IT infrastructure readiness of the library, computers are provided, at some or all location, for the following activities:

1. Accessing the Internet – includes full access and express stations, available with a signed agreement.
2. Workstations organized with topical indexes with access to pre-selected Internet sites and related information on popular subjects.
3. Educational games suitable for all ages.
4. Document preparation assistance through office applications (word processing, etc.) for enhanced productivity.
5. Online access to the library catalog.
6. Computer training seminars and workshops.
7. Computer laboratories to be used for training seminars, workshops and general computer use.

Many organizations may not have an explicit policy about use of mobile hand-held devices; the dangers from careless and unrestricted use of such devices are explained in Chapter 3. In view of that, the policy should indeed mention about such devices as they may contain a facility for wireless access as well.

Public Library Example

Unfiltered limited wireless Internet access is provided at some or all locations. It is free of charge for patrons provided they have the required hardware and software needed for this service:

1. Access is provided on a first connect basis and controlled automatically by the access point.
2. It is the owner's responsibility to set up their equipment to access the library's wireless network.
3. No responsibility is assumed by the library toward the safety of wireless network or for configurations, security or data files resulting from connection to the library's wireless service.
4. Library staff shall not configure users' device, nor shall they provide assistance in getting user device connected to the wireless network other than providing basic information needed for setup.
5. Security and protection from virus is the responsibility of the user.

Disciplinary Action for Privacy Violation and Disclaimer

These are the last two important sections of the safe computing policy.

Public Library Example

Disciplinary action against violators

Those who violate the Computer Usage Policy may lose Library privileges. Staff will also be subject to normal disciplinary procedures as well. Violations of the Policy for legal and ethical use of computing resources will be subjected to disciplinary action with due seriousness and in appropriate manner. Illegal acts involving Library computing resources may also be subject to appropriate legal authorities.

Disclaimer

The Internet is a global electronic network – as such, there is no control over users or website content. The Internet and its available resources may contain material of a controversial nature.

In abidance with the prevailing laws, library computers that connect to the Internet use a technology protection measure to filter and block access to images considered to be obscene, pornographic or harmful to minors. However, please note that filters and anonymizers may not be cent percent effective and as such, they may not be able to filter images that ought to be blocked. Conversely, anonymizers may block images that should not be blocked. In the event a site is wrongly blocked, or conversely, not blocked, library users have the provision to request review. It is mandatory that parents of minor children take the responsibility for their children's use of the Internet through the library's connection. Parents and local guardians are encouraged to supervise their children's/ward's use for surfing on the Internet so that the safety of children is ensured. The library shall not be responsible for the ill effects that may come upon children due to surfing on the Internet.

Library staff cannot control the availability of information links that often change rapidly and unpredictably. Not all sources on the Internet provide accurate, complete or current information. Users need to be adept at getting information from consumers, questioning the validity of the information.

Miscellaneous

For the sake of completeness of the policy, many other relevant points should also be specified; for example, how long the facility can be used, rules about any ancillary services provided, such as printing facilities, saving of user documents on the computer system and any other points that relate to the use of computers.

Public Library Example

Computer Usage Policy – Acceptable Use Agreement

1. Daily usage of computer is limited to 1 hour per session unless no one is waiting. Each individual is requested to curtail their use to 5 hours per week only so as to enable maximum use of computers across all users visiting the library.
2. Use of express station is available only on a first-come, first-served basis and only for short-term intervals. Please abide by this so that all users get equal opportunity.

Sign-in at service area information desk or PC reservation station

1. As a user of this facility, you need to sign-in at the information desk or PC reservation station for use of all library computers except the online catalog and the topic-specific workstations.
2. Computer user voucher card or receipt will be provided to you. You are requested to return the voucher card to the desk at the end of your computer usage.
3. Users of full access Internet stations must use either their own current library card or their own current guest card issued by the Library. Photo identification can be used to verify the identity of a registered user if necessary. Please make appointments in person or on the phone for hour long sessions. Print only if you must and use two-sided printing feature when you print.

Printing services at the library

There is charge levied for use of printing facility. These charges may be revised from time to time as appropriate in the prevailing circumstances. Use the "print preview feature" to view before printing – this helps minimize paper use.

Saving of user files and use of computers at the library

You must always save your work on removable media and not the hard drive. Removable media should be scanned before the computer is in use. You can purchase removable media at the desk-subject to availability. No external software program will be allowed to use – use only software program that the library has installed. All minors who use full access Internet must have their parent's or legal guardian's signature granting permission on the Fontana Regional Library Application for Borrower's Card or the Fontana Regional Library Acceptable Use Agreement.

Help

Please ask the library staff for help if you have any problems accessing the Internet, computer software or printing.

A very important point is that an organization must ensure that its users/employees sign the agreement for safe commuting.

Public Library Example

Agreement

I understand that there is detailed information in the *Library Computer Usage Policy on Confidentiality, User Responsibilities* (including ethical, legal and parental responsibilities), a *Disclaimer* about information on the Internet, and possible sanctions when users violate the policy.

I hereby agree to comply with the stated rules of the policy. My signature affixed here is to indicate that I have accepted the policy and usage within its boundary.

Print Name _____ Date _____ Guest []

Signature _____ Staff initials _____

Parent's Signature for Minors _____

- I give my child permission to use the Internet at the library.
- I do NOT give my child permission to use the Internet unless it is surfing under my supervision.

A complete example template for computer and network usage policy is provided in Appendix C – Part II (in CD).

9.9 Incident Handling: An Essential Component of Cybersecurity

The topics addressed in this section are – definition for (cyber) security incident, example of incidents, the need for incident response handling systems, recommended best practices in this area, the benefit from having an incident handling and incident response systems and structuring the incident response teams. Refer to Part II of Appendix D – it is also mentioned in Section 9.9.8.

9.9.1 Definitions and Entities Involved

The discussion here applies to security incident in general as well, that is, not necessarily to “cyber-security” incident in particular. Precisely defining incident management is difficult; the words mean different things to different professionals. For example, in the Information Technology Infrastructure Library (ITIL), a best practice series of books providing guidance on developing and implementing quality information technology (IT) services, “incident management” refers to the handling of any type of service disruption or interruption. The scope of definition for incident management provided here includes preventing and handling computer security incidents. This includes identifying and minimizing the impact of technical vulnerabilities in software or hardware that may expose computing infrastructures to attacks or compromise, thereby causing incidents. Part of the inherent difficulty in defining the term “incident management” is defining the term “incident,” which is often derived based on organizational requirements and specifications. An incident is defined as “the act of violating an explicit or implied security policy.” SANS definition is “an adverse event in an information system, and/or network, or the threat of the occurrence of such an event.” For the context of this section, the definition of a computer security incident is: “*any adverse event which compromises some aspect of computer or network security.*” The definition of an “event” is: “*an occurrence in a system that is relevant to the security of the system.*” We use the word “event” to describe activity that is computer security related but that has not

yet been identified as an incident or vulnerability. From legal perspective, the notable feature of the 2008 amendment is that it has attempted to bring in comprehensive information security to the IT industry. A new term *Cybersecurity* under Section 2(nb) has been added to the Act. It has been defined as follows: “*Cyber Security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.*” The said definition provides security in terms of both physical security to the devices and security to the information stored therein such devices. The said definition provides protection from unauthorized access, use, disclosure, disruption, modification and destruction to both physical device and the information stored therein.

The three important terms: “incident response,” “incident handling” and “incident management” have a relationship among them. Often people are not clear about the relationship (see Fig. 9.11) and these three terms are used interchangeably.

The next important point to address is “who is responsible for performing incident management activities?” Typical answers would be (a) Computer Security Incident Response Team (CSIRT); (b) IT (the information technology group) or (c) the security group. However, considering the deeply embedded role of IT into business, the global scenario and complexity of cyberattacks, it is seen that effective incident management

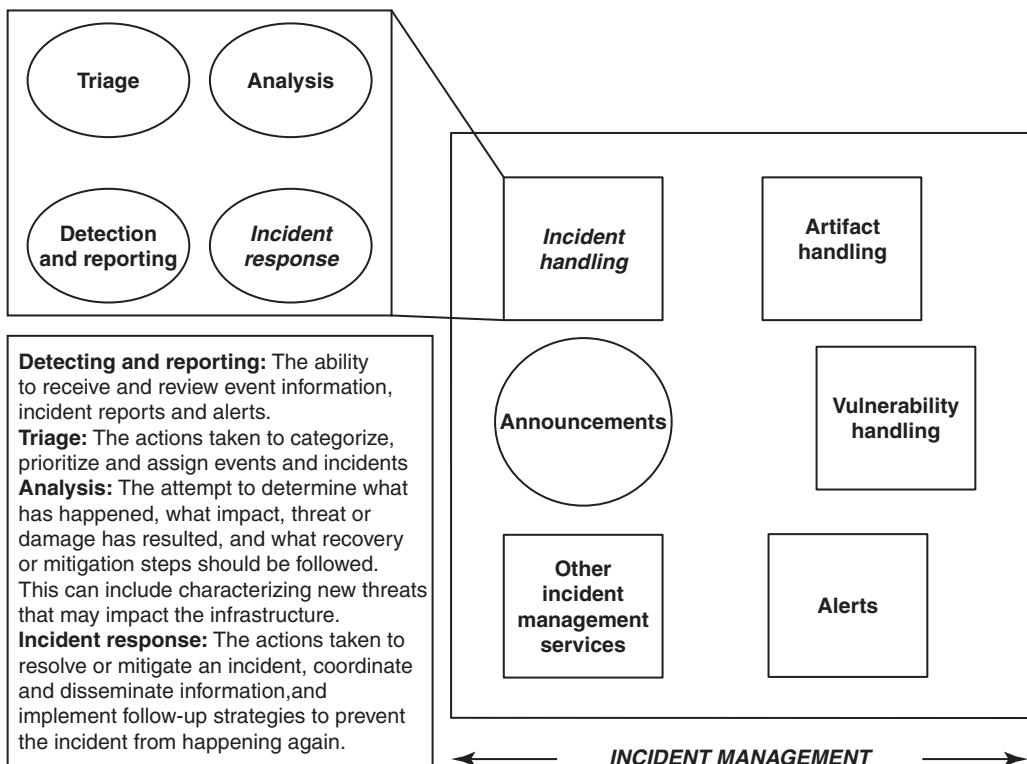


Figure 9.11 | Incident response, incident handling and incident management – the relationship.

includes participants from outside these areas. For example, some very specific processes related to incident management may be performed by

1. The HR team, who participates in separating an employee found to have been performing malicious computer activity.
2. Legal team who may provide interpretations of rules and regulations and their impact on implementing security policies and practices or who may be called for help to determine organizational liability when internal systems are being used for malicious activity.
3. The firewall manager who puts certain filters in place to prevent a denial-of-service attack from continuing;
4. An outsourced service provider repairing systems that have been infected with a virus.

Management of legal issues involving CSIRT teams is not to be underestimated. It means coherent view should be taken about the legal issues faced by incident response team. Legal advice should be taken from legal experts who are experienced in this area and understand technical terminology and issues that form the basis of daily CSIRT work. It is important that legal advisors are enlisted on a long-term basis, that is, years instead of months, because the amount of domain-specific knowledge needed should not be underestimated. A practical and cost-effective solution can be used by the legal advisors of your parent organization, but only when these people are experienced enough to guide you through your specific problems. If the legal staff does not fit this need, then you might have to hire or retain a lawyer that better fits your specific requirements, if it is feasible. There could be more entities than mentioned in Fig. 9.12.

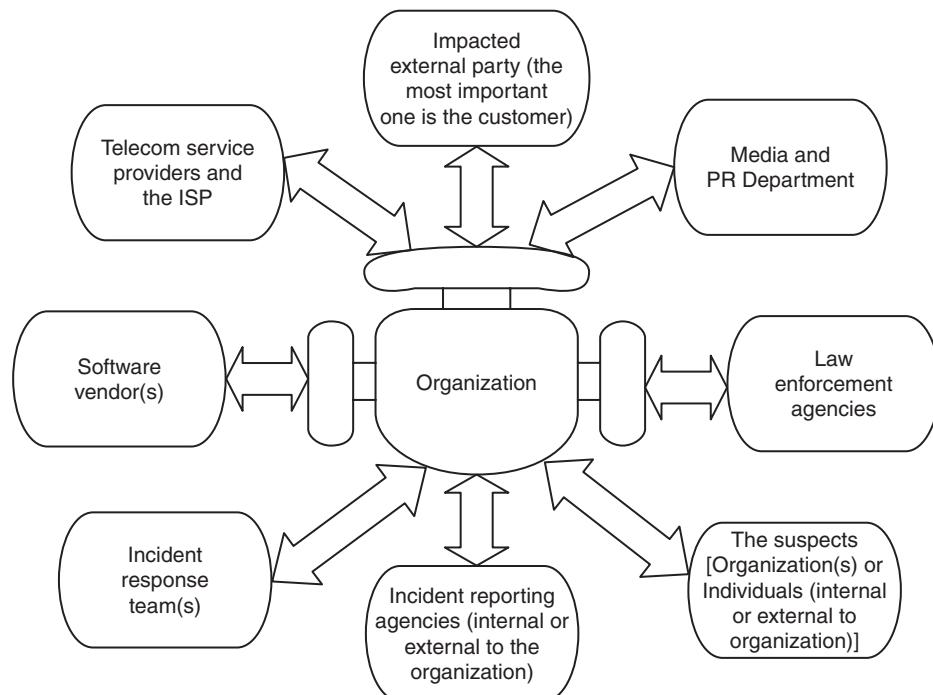


Figure 9.12 Entities involved in incident-related actions and communication. Here ISP is Internet Service Provider and PR implies public relations.

As a cardinal principle in incident handling – “incidents” should be classified so that the Pareto principle can be applied; remember that there is always a cost attached to an incident investigation, reporting and closure. Incidents include but are not limited to the following list:

1. Loss of computing devices (such as laptops, hard disks, portable storage devices, etc.).
2. Detection or discovery of a program agent including, but not limited to, viruses, worms, Trojan Horse programs, keystroke loggers, rootkits, logic bombs, Spam relays, remote control Bots (discussed in Chapters 2 and 4).
3. Detection or discovery of unauthorized users, or users with privileges in excess of authorized privileges.
4. Detection or discovery of critical or widespread vulnerabilities, or mis-configuration that can lead to a compromise affecting the “confidentiality,” “integrity” or “availability” of information (C.I.A. are the three pillars of information security).

We can also give a risk perspective to the cybersecurity incidents: (a) High-risk incident and (b) low-risk incident. An incident is high risk when it meets one of these following criteria:

1. Involves a keylogger, rootkit (see Chapter 7), remote access agent, password cracking agent or a new threat from an unknown vector (addressed in Section 2.7, Chapter 2) or
2. Involves a server with the loss of confidential or operationally critical data.

An incident is low risk if it does not meet the criteria of a high-risk incident. Following are some examples that may indicate security incidents:

1. A system alarm or equivalent indication from a tool installed for intrusion detection.
2. Suspicious entries in system or network accounting (e.g., a Unix user obtains root access bypassing the normal sequence necessary to obtain this access).
3. Accounting discrepancies (e.g., someone notices a few minute gap in the accounting log in which no entries whatsoever appear).
4. Unsuccessful logon attempts.
5. Unexplained, new user accounts.
6. Unexplained, new files or unfamiliar file names.
7. Modifications to file lengths and/or dates, especially in system executable files – all without explanation.
8. Attempts to write to system files or changes in system files without any explanation or rationale for use.
9. Unexplained modification or deletion of data.
10. Denial-of-service (DoS) or inability of one or more users to login to an account system crashes.
11. Degradation in system performance.
12. Operating a program in an unauthorized manner or unauthorized use device to sniff network traffic.
13. “Door knob rattling” (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts etc.).
14. Unusual time of usage (remember, more security incidents occur during non-working hours than at any other time).
15. An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user.
16. Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program).

Note: There is a caveat – this list is not exhaustive. Moreover, not a single incident mentioned in the list is a typical symptom of security incidents nor it is generally conclusive by itself. Therefore, observing one or more of these symptoms should prompt you to investigate events more closely. It is better to work with other personnel at your organization who possess the appropriate technical and computer security knowledge to determine exactly what has occurred. When it comes to identifying incidents, collective judgment works better than a single person's judgment.



Data breaches are very common these days and therefore *data incidents* should not be forgotten.

See Fig. 9.11 – an end-to-end incident management system involves several phases – incident notification, incident recording, incident investigation and analysis, presentation to concerned management team members, and finally closure with mitigation actions put in place and lessons learnt recorded in organization's database. In practice, incident handling and management is not simple – it can be a tricky situation, more so when an organization is large and complex. When the external affected entity is the end customer, nasty escalations flow. Figure 9.12 shows the multiple stakeholders involved in actions and communication relating to incident.

Some more key terms to note are: (a) “incident” – in general, (b) “data incident” – in particular and (c) “cybersecurity incident.” A potential “data incident” is a suspected loss or theft of data, or loss or theft of media or misuse of data or disclosure of data or access to data by an unauthorized third party or an inability to locate portable media in inventory. In this section, the terms “incident” and “computer security incident” are used interchangeably. The term “incident” is very important and there are multiple definitions available for this term. “Event” and “adverse events” are the two related terms to be noted. We can say that an *event* is an observable occurrence in a system or network. For example, events include a user connecting to a file share, a server receiving a request for a webpage, a user sending E-Mail and a firewall blocking a connection attempt. All events may not call for a countermeasure unless they are “adverse events” which sometimes are referred to as “risk events.” *Adverse events* are events that result in negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to “sensitive data” and execution of Malicious Code that destroys data (recall the discussion in Section 9.2 about this). This section addresses only adverse events that are related to computer security and excludes adverse events caused by sources such as natural disasters and power failures. Note that a computer security incident is a violation or imminent “threat” of violation of computer security policies, Acceptable Usage Policy or standard security practices. Figure 9.13 helps relate the key terms mentioned (event, risk and threat, etc.).

Often incident reporting systems and associated metrics can get into trouble if the stakeholders involved are not clear about these terms. Another simple scheme for classification of incidents could be as follows:

1. IT security incident

- Inappropriate usage of organizations' assets/resources.
- Tampering with IT controls (e.g. disabling firewall, stopping antivirus service, making changes to group policy).
- Unauthorized changes of IT systems without an appropriate change request.
- Spam and mail forgery.
- Use of unlicensed software/tools/applications.

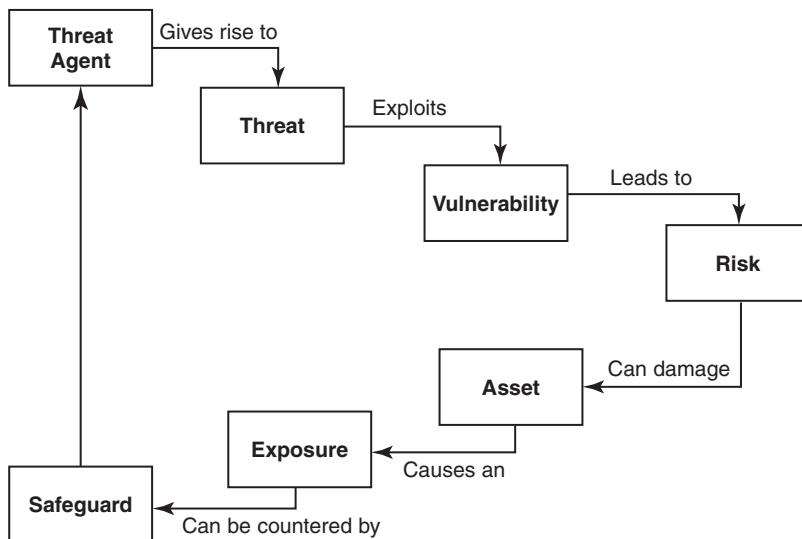


Figure 9.13 | Threats, vulnerabilities, assets and risks.

- Downloading inappropriate materials.
 - All instances of successful infection or persistent attempts at infection by Malicious Code, such as viruses, Trojan Horses or worms (multiple workstations, users, servers, etc.).
 - Denial-of-service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more large portions of a network.
 - Unauthorized sharing/misuse of system/application/tool password sharing, wherein someone performs certain tasks on behalf of somebody else or/and view the information.
2. Data incidents/data privacy incidents:
- All instances of the loss of, theft of, missing, unattended storage device (laptop, hard disk, portable media, USB, CD, etc.).
 - Loss/theft of confidential data, client information, company confidential information.
 - Serious loss of organization's classified information, espionage, eavesdropping and other means of obtaining sensitive information illegally.
 - Unauthorized disclosure/sharing/misuse of organization data/client information (posted on public website, passed on as a paper document, verbally or by electronic media, technical information about current or planned products or processes cost, pricing, sales, marketing or service strategies).
 - Misuse of customer PI/SPI. PI is the information that identifies, or can be used to identify, contact or locate the person to whom such information pertains. PI consists of two components: an identifier and an attribute. SPI is information that could be misused to harm a person in a financial, employment or social way.
 - Misuse of credit card information (see Section 11.4.1, Chapter 11 has illustrative examples on this).
 - Manipulating customer E-Mail address for ill purposes.

- Changing PI/SPI of the customer (address, E-Mail address, date of birth, card details, etc.) without consent of the customer.
- Unauthorized sharing/misuse of customer/client passwords that may risk compromising their PI/SPI.

Incident classification, in terms of “high risk” and “low risk” was mentioned earlier. *Priority* of an incident is determined by the combination of *urgency* and *impact* of the incident, for example, “priority” is “low” for an incident whose “urgency” and “impact” are both low and “priority” is “high” for an incident whose “urgency” and “impact” are both high. Here is a generally accepted scheme used in industry for priority levels for risks arising from incidents.

Critical priority means an instantaneous and continued effort using all available resources until resolved. Here on-call procedures are activated and vendor support is invoked;

1. **High priority incidents:** These that have a huge impact on the organization’s business or service to customers. For such incidents, technicians/incident response management team member(s) must respond immediately. He/she must assess the situation and he/she may interrupt other staff working low or medium priority jobs for assistance. For example, Malicious Code attacks including Trojan Horse programs and virus infestations, and unauthorized system access.
2. **Medium priority incidents:** These have a significant impact or have the potential for a huge impact on the organization’s business or service to customers. For such incidents, technicians/ incident response management team member(s) can respond using standard procedures and operating within normal supervisory management structures. For example, password cracking attempts, situations in which password does not allow access to system and apparent change of password without user knowledge has occurred.
3. **Low priority incidents:** These have the potential to have a significant or monumental impact on the organization’s business or service to customers. For such incidents, responding using standard operating procedures when time allows. For example, probes and network mapping and denial of access to the system due to unexpected lockout.

The scope of incident management for the discussion here is computer security incident management (referred to as “incident management”). We should distinguish between “security management” and “incident management,” especially, when the scope of incident management includes processes for protecting infrastructures and detecting events using network monitoring and IDS. The boundary between the two is open to interpretation and can be confusing. The dividing line often depends on the structure of an organization’s security or incident management capabilities. Incident management processes fall within the scope of security management (see Fig. 9.14).

9.9.2 Why should Organizations have Incident Response Systems?



With the rising number of threats in the cyberspace, there is indeed a strong need for instituting incident response management systems in organization.

Incident response has become necessary because cyberattacks frequently cause the compromise of personal and business data. Many times, they compromise privacy of data as well as personal privacy

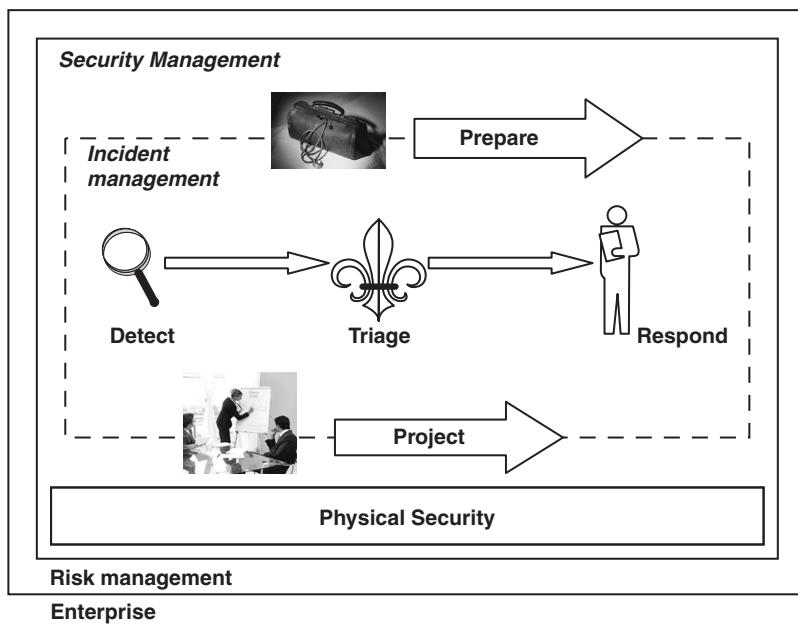


Figure 9.14 | Incident management and security management.

of individuals. There have been real incidents involving viruses, worms, Trojan Horses, Spyware and other forms of Malicious Code – all of them have disrupted or damaged millions of systems and networks around the world. Much about that has been explained. There are also illustrative examples presented about this in Chapter 11 (in CD). Serious concerns about national security and exposure of personally identifiable information (PII) are also raising awareness of the possible effects of computer-based attacks. These events and many more events make the case for responding quickly and efficiently when computer security defenses are breached. To address these threats, the concept of computer security incident response has become widely accepted and implemented in the Federal Government, private sector and academia. One important point to appreciate is that incident management is *not* same as security management; it is only a part of security management (see Fig. 9.14).

9.9.3 Examples of Cybersecurity Incidents and the ITIL Perspective

Examples of incidents are mentioned in Table 9.2 they are also discussed in other chapters of the book as mentioned in the last column of the table). An important point to note is: An “imminent threat of violation” means a situation wherein the organization has adequate facts to believe that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of a new worm that is rapidly spreading across the Internet – this is mentioned in one of the examples in Table 9.2. In practice, incident response teams typically handle many Acceptable Usage Policy violations.

Table 9.2 | Cybersecurity incident examples

<i>Incident Example</i>	<i>Explanation</i>	<i>Other Chapters in the Book for Additional Discussion</i>
Unauthorized access	An attacker runs an exploit tool to gain access to a server's password file. A perpetrator obtains unauthorized administrator-level access to a system and the sensitive data it contains, and then threatens the victim that the details of the break-in will be released to the press if the organization does not pay a designated sum of money.	Chapters 1 and 11 (case illustrations)
Inappropriate Usage	A user provides illegal copies of software to others through peer-to-peer file-sharing services. A person threatens another person through E-Mail.	Illegal copies of software falls under Intellectual Property Rights (IPR) crime, that is, violation of IPR. Chapter 11 has some case illustrations on this. See Chapter 6 for legal aspects involving IPR crimes
Denial of service	An attacker sends especially crafted packets to a web server, causing it to crash. An attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization's network.	Chapters 1, 2 and 4
Malicious Code	A worm uses open file shares to quickly infect several hundred workstations within an organization. An organization receives a warning from a vendor of an antivirus package. The vendor informs the organization about a new worm spreading rapidly via E-Mail throughout the Internet. The worm takes advantage of a vulnerability that is present in many of the organization's hosts. On the basis of previous antivirus incidents, the organization expects that the new worm will infect some of its hosts within the next 3 hours.	Chapters 2 and 4 (worms, viruses, Trojans, etc.)

Box 9.8 Malware Incidents

Malware incidents are a significant external threat to the security of many IT systems, often causing widespread damage and disruption, and forcing users and organizations to carry out extensive, costly efforts to restore system security. Malware includes five categories of inserted programs: (a) viruses, (b) worms, (c) Trojan Horses, (d) malicious mobile code and (e) blended attacks. Viruses and worms are usually designed to carry out their functions without the user's knowledge. Blended attacks use a combination of techniques to insert malicious programs. Malware also includes other attacker tools such as backdoors, rootkits and keyloggers, and tracking cookies that are used as Spyware. Spyware, when inserted into a user's system, threatens personal privacy and enables the attacker to monitor personal activities and to carry out financial fraud. Also see Box 9.2.

Refer to detailed discussion in Chapters 2 and 4 where malware, virus, worms and Bots are discussed – also see Box 4.3 about "malware" and "Trojan Horses" and Box 4.8 about "blended threat."

Table 9.3 | Summary of cybersecurity incidents handled by CERT-In

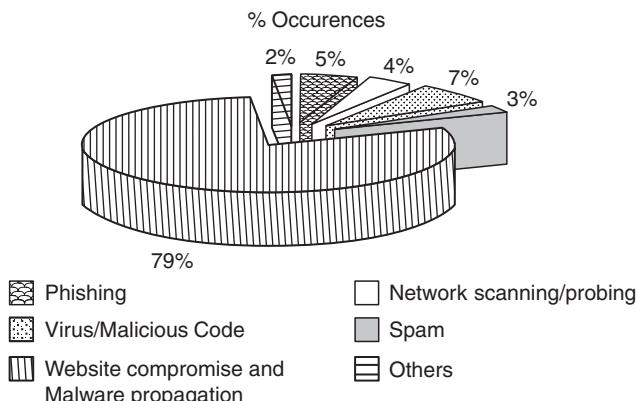
<i>Cybersecurity Incidents</i>	<i>2004</i>	<i>2005</i>	<i>2006</i>	<i>2007</i>	<i>2008</i>	<i>2009</i>
Phishing	3	101	339	392	604	374
Network scanning/probing	11	40	177	223	265	303
Virus/Malicious Code	5	95	19	358	408	596
Spam	—	—	—	—	305	285
Website compromise and Malware propagation	—	—	—	—	835	6,548
Denial of service	—	—	—	—	54	15
Others	4	18	17	264	94	145
Total	23	254	552	1,237	2,565	8,266

The year 2009 annual report of Computer Emergency Response Team – India (CERT-In) is the latest reported reference at the time of writing this. It clearly shows the sharp rise in the number of cybersecurity incidents year by year (see Table 9.3). Refer to link to this report in Ref. #18, Additional Useful Web References, Further Reading.

Thus, in the year 2009, CERT-In handled more than 8,000 incidents. The statistics by percentage break-up of the categories of cybersecurity incidents handled by CERT-In are presented in Fig. 9.15.

9.9.4 What Organizations Can Do To Protect their Systems from Cybersecurity Incidents?

The numbers in Table 9.3 indicate the sharp rise in cybersecurity incidents – organizations need to protect their information systems from malware through their ongoing IT security planning, management and implementation activities. Organizations also need to protect business-sensitive information in general and protected health information (PHI) in the healthcare sector, and PI and SPI of their multiple stakeholders. Stakeholders typically are employees, clients, end customers of the clients (whose personal/sensitive information may be entrusted with the organization in the processing that is involved within the scope of delivery work), contractors and consultants with whom the organization may be dealing with.

**Figure 9.15** | Statistics – incidents handled by CERT-In (categories).

9.9.5 Best Practices for Organizations

As part of cybersecurity best practices, organizations should consider the following actions in particular against the threat of malware (see Chapters 2 and 4):

1. Develop and implement an approach to *malware incident prevention* based on the attack methods (known as “attack vectors” mentioned in Chapter 2) that are most likely to be used, both currently and in the near future. Choose prevention techniques that are appropriate to the computing environment and system, and provide for policy statements, awareness programs for users and IT staff, and vulnerability and threat mitigation efforts.
2. Develop and implement policies that support the prevention of malware incidents. Conduct ongoing awareness programs for user and IT staff. Ensure vulnerability mitigation, and security tool deployment and configuration. Malware prevention should be stated clearly in policies, which should be as general as possible to allow for flexibility in implementation and to reduce the need for frequent updates. Policy statements should be specific enough to make their intent and scope clear and to achieve consistent and effective results. An often forgotten target is the remotely working population in an organization. Therefore, policies should address provisions that are applicable to remote workers, both those using systems controlled by the organization and those using systems outside of the organization’s control such as contractor computers, home computers, computers of business partners and mobile devices.
3. Incorporate prevention of malware incident and handling of awareness programs, and provide guidance and training to users. Users should be alerted to the ways that malware spreads, the risks that malware poses, the inability of technical controls to prevent all incidents and the role of users in preventing incidents. Users should be aware of policies and procedures for incident handling, including how to detect malware on a computer, how to report suspected infections, and what can be done to assist the incident handlers.
4. Establish capabilities to mitigate vulnerabilities and to help prevent malware incidents through documented policy, technical processes and procedures. Appropriate techniques or combinations of techniques should be used for patch management, application of security configuration guides and checklists, and host protection to address vulnerabilities effectively.
5. Establish threat mitigation capabilities to assist in containing malware incidents by detecting and stopping malware before it can affect systems. National Institute of Standards and Technology (NIST) strongly recommends that organizations install antivirus software on all systems when such software is available. Other technical controls that can be used are IPS, firewalls, routers and certain application configuration settings.
6. Establish a robust incident response process capability that addresses malware incident handling through preparation, detection and analysis, containment/eradication/recovery and post-incident activities.
7. Establish malware incident prevention and handling capabilities that address current and short-term future threats that are robust and flexible. Maintain awareness on the latest threats and the security controls that are available to combat each threat. Plan and implement appropriate controls, emphasizing the prevention of malicious incidents.

The use of malware, Spyware (see Chapters 2 and 4), Phishing attacks (Chapter 5), and other attempts to collect PI are expected to lead to future Identity Theft (discussed in detail in Chapter 5) and financial frauds (refer to Chapter 11). The development of more robust Spyware detection and removal utilities, and more effective antivirus software should be driven by demands for better protection. There is a “catch 22” issue involved – better technical controls could make attackers even more resourceful and innovative in avoiding

automated detection and taking advantage of the trust of users. There are viruses and worms that could attack PDA devices and cell phones, or that could use these devices as malware carriers. Given the trends in workforce mobility, this is a cause for concern because PDAs and other hand-held Wi-Fi devices are used heavily by mobile workers. Organizations must, therefore, be aware of the latest threats and should be prepared to implement appropriate security controls to protect their IT systems. With regard to this, please refer to Section 8.8 of Chapter 8 from forensics perspective.

Incident handling process is a complex one and involves several phases as well as multiple stakeholders (see Figs. 9.11 and 9.12). The components/phases of an incident response process are explained in Table 9.4.

Table 9.4 | Incident response process – phases/components

<i>Process Phase/Component Name</i>	<i>Brief Description</i>
Preparing for incident response	<ul style="list-style-type: none"> • To be ready for this, develop malware-specific incident handling policies and procedures. • Also conduct regular training and exercises geared to malware handling. • Assign a few individuals or a small team to be in charge for coordinating the organization's responses to malware incidents. • Establish an organization-wide strong communication mechanism so that coordination among incident handlers, technical staff, management and users can be sustained if an attack occurs (see Fig. 9.12 – it shows the entities involved).
Detecting, classifying, recording and getting ready for initial support	<ul style="list-style-type: none"> • Continuously monitor malware advisories and alerts produced by technical controls, such as antivirus software, Spyware detection and removal utilities, and IDS, to identify impending malware incidents.
Analyzing the incident and the diagnosis	<ul style="list-style-type: none"> • Review malware incident data from primary sources. Such inputs typically come from user reports, IT staff reports and technical controls to identify malware-related activity. • Use trusted toolkits on removable media that contain up-to-date tools for identifying malware, listing currently running processes and performing other analysis actions. • Establish priority levels to identify the appropriate level of response for various malware-related incidents.
Containment	<ul style="list-style-type: none"> • Ascertain the authority to make major containment/resolution decisions. • Decide the timelines for appropriate actions and the methods of containment that will be employed. <p><i>Note:</i> Early containment/resolution can help stop the spread of malware and prevent further damage to systems. Strategies and procedures for making containment-related decisions should reflect the level of risk acceptable to the organization.</p>
	<ul style="list-style-type: none"> • Instruct users about how to identify infections and what measures to take if a system is infected. However, do not rely primarily on users for containing malware incidents. Use updated antivirus software and other security tools to contain incidents. • Take your security software/solution service providers and vendors into confidence – submit copies of unknown malware to them for analysis and contact trusted parties, such as incident response organizations and antivirus vendors, when guidance is needed on handling new threats.

(Continued)

Table 9.4 | (Continued)

<i>Process Phase/Component Name</i>	<i>Brief Description</i>
	You may need to shutdown or block services such as E-Mail or Internet access to contain a malware incident and understand the consequences of doing so. Be ready for this eventuality!
Eradication	<p>Also be prepared to respond to problems caused by other organizations disabling their own services in response to a malware incident. Identify those hosts infected by malware, considering users who have remote access to systems and mobile users.</p> <ul style="list-style-type: none"> • To remove malware from infected systems, you may need to use combinations of eradication techniques at the same time for different situations. • You will need to support awareness activities to inform users about eradication and recovery efforts.
Resolution and recovery	<ul style="list-style-type: none"> • Restore the functionality and data of infected systems and lift temporary containment measures. • Think about possible worst-case scenarios and determine recovery plans under those scenarios, including rebuilding compromised systems from scratch or from known good backups. • Determine when to remove temporary containment measures, such as suspension of services or connectivity. • Containment measures should be available until the number of infected systems and systems vulnerable to infection is sufficiently low that subsequent incidents should be of little consequence. • The incident response team should assess the risks of restoring services or connectivity and report to organization managers, who are responsible for assessing the business impact of maintaining the containment measures and for determining actions to be taken concerning containment.
Post-incident activity	<ul style="list-style-type: none"> • Conduct an assessment of lessons learned after major malware incidents to prevent similar future incidents. • Identify the required changes to security policy, software configurations and the implementation of malware detection and prevention controls. <p><i>Note:</i> The activity does not stop after resolution and recovery.</p>

Figure 9.16 summarizes the incident response life cycle based on the activities described in Table 9.4. ITIL is a set of IT best practices seen from ITIL perspective; the activities of incident management constitute the following:

1. Taking the ownership for an incident and acting as the single point of contact (SPOC) for first-level escalation.
2. Providing a prompt recovery of the business within the specified or Service Level Agreement (SLA).
3. Ensuring continued focus (till closure) on the incident resolution.
4. Incident escalation: (a) functional escalation for getting the support of a higher technical skill to reach problem resolution and (b) hierarchical escalation – to consult a manager with more authority so that the right kind of decisions are taken.
5. Sending incident notifications to the affected entities so that they have the latest status information.
6. Setting-up and leading conference call or communicating with all involved parties (refer to Fig. 9.12).

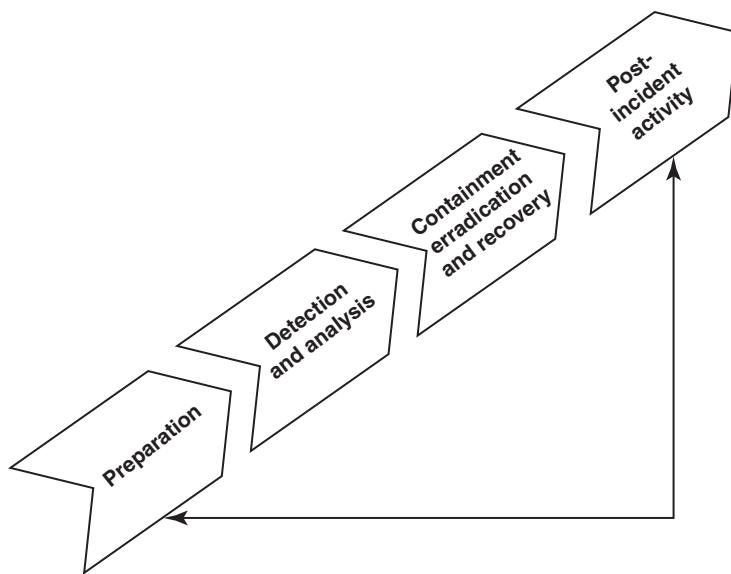


Figure 9.16 | Incident response life cycle.

7. Continuous tracking and recording of the timelines on resolution.
8. Acting as an interface with other technicians, customer technical staff and other groups within the organization.

Once the incident has been resolved, the impetus should not stop only there. The concerned team with management direction and guidance should get into a root cause analysis mode after studying if there is a “pattern” in the incidents. For this, the organization’s “lessons learned” database is useful if the past incidents are diligently recorded. Ultimately, it may call for “penetration testing” and “vulnerability scanning” exercises. For a detailed discussion on this, refer to Ref. #6, Books, Further Reading.

9.9.6 Incident Response Team Work, Capabilities and Structure



Guidance on incidence response team structuring is provided in Appendix H (in CD).

Once an organization decides that it needs active management and response to cybersecurity incidents, an active coordination and management role needs to be created. Simply stating that “security is everyone’s responsibility” will not work. Therefore, incident response team needs to be formed. We just discussed the complex tasks and activities involved in incident handling (see Table 9.4). Staffing the incident response team is a tricky issue in reality because incidents may not occur daily and therefore IT management would be reluctant to bear the cost of the team in their operations budget. Whether the team for handling security incidents should be employed on a full-time basis or a part-time basis has become a debatable issue.

Team success is about skills, competencies, capabilities and training. Haphazard teams with inadequate skills will not work. Often you might hear the term “incident response” being equated with the term

“incident response team.” Although this might appear OK, it is not correct. It is because of the “skills and competency” view point mentioned – people who know little or nothing about the process of incident response often become involved in dealing with security-related incidents. A classic example is of users in most organizations.

Let us consider a situation wherein a worm infects numerous systems. Users might collaborate to analyze what went wrong and they may even decide to eradicate the worm. Even then, they can hardly be called an incident response team. This is because an incident response team is a “competency-based capability” responsible for dealing with potential or real information security incidents. A team is assigned a set of duties related to bringing each security-related incident to a conclusion. This ideally should be in accordance with the goals of the organization to which it provides service – recall the components and phase of incidents handling mentioned in Table 9.4. There is, therefore, a difference between individuals who are dealing with an incident and an incident response team which is mission-based. Such a team works on the basis of job-related responsibilities for each team member. Although individuals might sometimes become involved (out of their own initiatives) in dealing with incidents, it is an incident response team that is assigned the responsibility of dealing with incidents as part or all of the job descriptions of the individuals involved.

People often wonder as to how many individuals must be involved in an incident response effort for them to collectively be considered a team. We know that a team consists of one or more individuals. One individual can effectively serve as the coordinator of efforts by a number of people. When incident handling efforts are finished, the others involved in the incident are released from any responsibilities they might have had in dealing with incident. However, the team member has the ongoing, day-to-day responsibility of handling incidents and will need to be ready for dealing with the next incident that may occur in the future. One practice that authors have found useful is the creation of diagnostic matrix to enhance skills of the team members. Such a matrix was found to be particularly useful for junior team members. When you create a diagnostic matrix for less experience staff, it becomes a reusable learning asset for the entire organization. An example of a diagnostic matrix is provided in Table 9.5.

Our work experience shows that such a matrix is helpful to helpdesk staff, system administrators and others who perform their own analysis of precursors and indications. It will also be helpful for new intrusion detection analysts and incident response team members. In the table, potential symptoms are listed on the left side and across the top there are incident categories. The cell entries within the matrix indicate which symptoms are typically associated with each incident category and how strongly that symptom is associated with the category. The matrix provides advice for less experienced staff members who may see the symptoms but cannot identify the likely underlying cause. The matrix also can be used as a training tool and can be enhanced by providing some supporting text, such as a brief justification of each matrix entry and advice on how to validate each type of incident.

Table 9.5 | Diagnostic matrix example

Symptom	DoS	Malicious Code	Unauthorized Access	Inappropriate Usage of Computing Resources
Files, inappropriate content	Low	Medium	Low	High
Files, critical, access attempts	Low	Medium	High	Low
Port scans, OUTGOING, unusual	Low	High	Medium	Low
Port scans, INCOMING, unusual	High	Low	Medium	Low
Host crashes	Medium	Medium	Medium	Low
High bandwidth utilization	High	Medium	Low	Medium
High E-Mail utilization	Medium	High	Medium	Medium

9.9.7 Benefits from Incident Response Systems

So far we have explained a number of key points – what is an incident, how to categorize incidents, the phases in incident response systems, teaming aspects for the incident response team best practices for cybersecurity incident handling, etc. Figure 9.17 shows the overall process flow in a typical incident response management system.

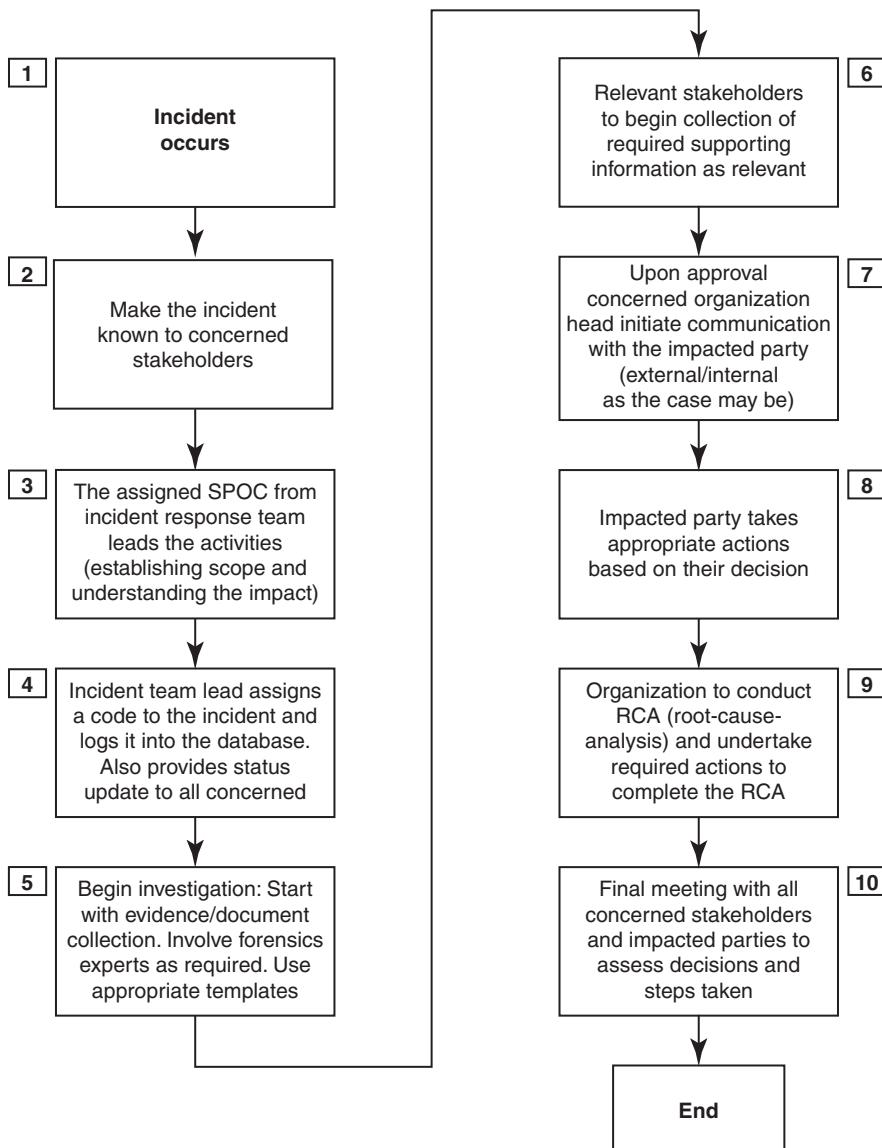


Figure 9.17 | Process flow: Incident response management system.

There are a number of benefits that follow from implementing an effective incident response system; the main advantages include:

1. Organization has the ability for responding to incidents systematically so that the appropriate steps are taken.
2. There is a provision for helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services. This results in timely resolution of incidents, resulting in reduced business impact.
3. Being able to use the information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data.
4. The ability to deal properly with legal issues that may arise during incidents.
5. Improved user satisfaction.
6. More efficient utilization of service desk and other staff.
7. Enhanced ability to measure and monitor IT performance relative to SLAs.
8. Better data to support executive decisions regarding service quality.
9. Improved ability to track incidents and service requests efficiently.
10. Proactive identification of process enhancements.



Every time there is an incident, it is a lesson for the organization to realize that possible security weakness may exist.

A systematically installed incident handling system makes it imperative for organization to carry out a root cause analysis of the incidents that have occurred. It also helps to study if there is a “trend” and “pattern” in the cybersecurity incidents that have taken place. Lessons learned from meetings provide other benefits. Reports from these meetings are good material for training new team members by showing them how the experienced team members respond to incidents. Information regarding an incident may be recorded in several places. Organizations should deploy centralized logging servers and configure devices to send duplicates of their log entries to the centralized servers. The team benefits because it can access all log entries at once and also, changes made to logs on individual hosts will not affect the data already sent to the centralized servers. A log retention policy is important because older log entries may show previous instances of similar or related activity. See Table D.II.13, Appendix D (in CD).

A system enforces recording of the information with regard to an incident. Such information is typically recorded in several places, such as firewall, router, network IDS, host IDS and application logs. With an incident response system in place, organizations are encouraged to deploy one or more centralized logging servers and configure logging devices throughout the organization to send duplicates of their log entries to the centralized logging servers. Incident handlers benefit from this practice because they have the pertinent log entries available together. This consolidation also provides secure storage for logs, which reduces the impact of attackers disabling logging or modifying logs on individual hosts that they compromise. In addition, creating and implementing a log retention policy that specifies how log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. Another reason for retaining logs is that incidents may not be discovered until days, weeks or even months later. The length of time to maintain log data is dependent on several factors, including the organization’s data retention policies and the volume of data. Generally, log data should be retained for at least a few weeks, preferably for at least a few months.

Use of checklists helps to harmonize the incident response analysis. In Appendix D, we have provided some checklists. It should be remembered always that checklists are merely to guide the team; a blind use of checklists will not help. Checklists need to be improvised from time to time based on usage experience. Refer to links on incident response related material in Ref. #18, Additional Web References, Further Reading.

9.9.8 Checklists

Checklists are useful in handling incident response work in the organization. A few checklists are and report templates provided in Appendix D. Following is the list:

1. Checklist for initial handling of incident.
2. Generic checklist for incident handling.
3. Checklist for handling DoS incident.
4. Checklist for handling Malicious Code incident.
5. Checklist for handling unauthorized access incident.
6. Checklist for handling inappropriate usage incident.
7. Checklist for handling multiple component incident.
8. Log review checklist for security incidents.
9. Computer incident reporting form.

Note that the checklists are based on type of incidents. Users may wish to use the checklists as their own choice. Users may also wish to suitably modify the checklists provided in Appendix D for appropriate usage in their context. However, they must also work with technically qualified security experts because checklist by itself is not the solution; it is only a tool to make the incident handling approach systematic.

9.10 Forensics Best Practices for Organizations

This section focuses on forensics readiness of organizations. For this section, the discussion in Chapters 7 and 8 is the essential background. The case illustrations provided in Section 11.6 of Chapter 11 should also be referred to after reading the discussion in this section.



Organization's forensics readiness is important – forensics readiness is defined as the ability of an organization to maximize its potential to use digital evidence while minimizing the costs of an investigation.

Preparation to use digital evidence is not easy – it involves system and staff monitoring, technical, physical and procedural means to secure data to evidential standards of admissibility, processes and procedures. All this becomes essential for ensuring that staff recognizes the importance and legal sensitivities of evidence, and appropriate legal advice and interfacing with law enforcement.



The prime factor in understanding the need for forensics readiness is a risk assessment.

Readers not familiar with risk assessment in information security context can refer to Ref. #12, Books, Further Reading. Standards such as ISO 27001 do emphasize on continuous risk assessment which is a valid starting point, but may not assess all the situations where digital evidence may be required. An asset register is certainly

needed to understand the attractiveness of targets to the types of crime such as fraud, malicious damage and IPR theft, as well as to understand the impact on the company if such an event should take place. However, be aware that any information security defensive measures based on a risk assessment will always leave a residual risk. Often this is because it is believed that users are insiders and therefore they will not cause a security incident. We know this is far from true – remember the “insider threats” discussed in the early part of this chapter.

From the discussion in Chapters 7, we learned that a forensics investigation of digital evidence is commonly employed as a post-event response to a serious information security incident. There can be many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs – remember the “chain of custody” principle explained in Chapter 7. The discussion in Section 9.9, about incident response management, is also relevant for discussion here. Many people believe that if an organization has a full-fledged information security department staffed with competent personnel and if there is also a dedicated incident response team, then the organization has a forensics readiness. This is far from true. Forensics readiness is incident “anticipation” compared with incident response. It means enabling the business requirement to use digital evidence. Information security, in general, concerns itself with ensuring that the business utility of information systems is maintained, and this includes ensuring that the business requirement for digital evidence is met.

It was mentioned in Chapter 7 that many forensic matter do not go to trial. The process of a digital forensics investigation (DFI) is subject to considerable scrutiny of both the integrity of the evidence and the integrity of the investigation process. Often, organizations tend to overlook this fact. They also tend to ignore what happens to the object of the investigation prior to the decision to undertake an investigation. The necessary evidence either exists, or hopefully it is found by the DFI, or it does not exist and a suspect cannot be charged and prosecuted. This is the law enforcement view of a DFI. It all begins when a crime has been committed or discovered and investigators attend a crime scene or wish to seize evidence. Unfortunately, all crimes that happen may not get reported and all crimes that are reported may not get investigated and ultimately, from the investigated cases, every suspect may not be brought to the court and even if that happens, the suspect may not be found guilty and therefore may not get sentenced to punishment (see Fig. 9.18).

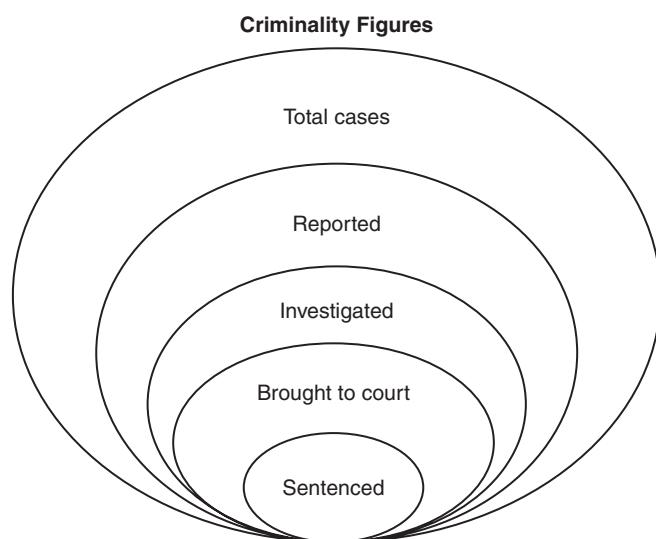


Figure 9.18 | Cyberforensics and case investigation: Where it ends.

9.10.1 Organizations must Understand Digital Forensics Investigation and Digital Evidences



Organizations must appreciate that the quality and availability of evidence is a passive aspect of the DFI.

Cybercriminals are known to exploit the fact that investigation is costly and takes time. Real-life situations show that half an hour of attacker time requires an average investigation time of 48 hours! (refer to the results found at <http://old.honeynet.org/challenge/results/index.html>). In a business context however, there is the opportunity to actively collect potential evidence in the form of log files, E-Mails, backup disks, portable computers, network traffic records and telephone records among others. This evidence may be collected in advance of a crime or dispute, and can be used to the benefit of the collecting organization. Going for litigation is generally a last resort for most businesses – if this is so then many organizations may ask why they should be concerned about potential evidence and related disputes.

Digital evidence could help manage the impact of some important business risks. It can support a legal defense; it could support a claim to IPR; it could show that due care (or due diligence) was taken in a particular process; it could verify the terms of a commercial transaction and it could lend support to internal disciplinary actions. There can be situations wherein a simple dispute or information security event may develop into a more serious one. For example, another organization notifies to your organization that your employee has released a virus into their network or says that your employee, according to that organization, has stolen source code that is their IPR. Imagine the ramifications of this situation especially if the other organization happens to be your competitor and suppose DFI indeed showed that such an act was done by your employee. If the evidence has not been gathered to begin with, it may be too late to do so later in the process. Therefore, it is necessary from the outset to consider the importance of evidence and to be prepared to gather it in anticipation of a wide range of scenarios.

Being in a position to gather and use evidence can also have benefit as prevention. A good deal of crime is internal – remember the two examples of “insider attacks” in Sections 9.1.1 and 9.1.2. Generally, employees will know organization’s attitude toward the policing of corporate systems. They will know, or will hear rumors, as to what type of crimes may have been successfully or unsuccessfully committed, and what action may have been taken against staff. A company demonstrating that it has the ability to catch and prosecute this type of insider attacker will dissuade them, much like the shop sign “We always prosecute thieves.” Information security programs often focus on prevention and detection measures. From a preventative information security perspective there is not much need for digital evidence. From a business perspective, however, there are a number of scenarios where collecting appropriate digital evidence would be beneficial. Thus, there is a business requirement for digital evidence to be available even before an incident occurs. The exact nature of this requirement is how the requirement is met and how organizations can make use of digital evidence. Understanding such aspects hardly gets addressed in organizations.

Most organizations would not have a separate policy for forensics, either due to lack of awareness about importance of computer forensics or due to budgetary issues. Once there is a policy, there is an expectation for its thorough implementation through policy-based procedures. If, however, there were to be a separate

forensics policy or mention of forensics in the overall security policy, then the categories of guiding procedures and activities that facilitate DFI are as follows:

1. Retaining information;
2. planning the response;
3. training;
4. accelerating the investigation;
5. preventing anonymous activities;
6. protecting the evidence.

Organization's approach to forensics should not be an isolated one. This is because, there is a strong link with the business continuity plan (BCP) and incident response procedures (recall the discussion in Section 9.9.6). The role of forensics procedures in an organization should fit within an overall security policy and strategy.

While preparing for forensics readiness, organization's should consider at least two objectives – first, maximizing an environment's ability to collect credible digital evidence – after all, the artifacts to be presented in the court should have the evidential integrity and should be acceptable in the court as discussed in Chapter 7 and secondly, minimizing the cost of forensics during an incident response. As learned from Chapter 7, there are several technical aspects in forensics – time-stamping, system hardening and compromised kernels. Some key factors that affect evidence preservation and investigation time are:

1. How logging is done;
2. What is logged;
3. IDS under use;
4. Forensics acquisition (of the evidence);
5. Evidence handling.

Those who are not familiar with intrusion detection system (IDS) can refer to Ref. #2, Books, Further Reading.

9.10.2 Concerns with Being a Forensically Ready Organization

An effective incident response system is pertinent to an organization's forensics readiness – this is because digital evidence is required whenever it can be used to support a legal process. An organization, therefore, needs access to the evidence that will be able to support its position in such an event. However, this is not easy as relevant evidence is unlikely to exist by default. In any computer security incident there is always a tendency to focus on containment and recovery because these are the foremost business critical issues. There is a trade-off to be made between recovery and evidence. A lot of information is also lost or discarded as part of normal business practice. To succeed in a legal process, it is therefore essential that the organization has actively gathered the evidence it is likely to require. Moreover, it is vital to have the capability to process evidence in a cost-effective manner, and to have suitably trained staff members who would ensure that potential evidence is preserved. The organization also needs to make appropriate and informed decisions in the light of the business risk. Besides this, organizations tend to have typical concerns when it comes to forensics. They are summarized in Table 9.6.

9.10.3 Key Activities for Organizations Getting Forensically Ready

In the context of forensic readiness discussion, the key activities are presented after Table 9.6 on the next page. Those are the activities that an organizations should consider if they wish to be forensically ready:

Table 9.6 | Forensics readiness – organizational concerns

<i>Forensics-related Concern / Apprehensions</i>	<i>Remarks</i>
There is a wide range of crimes and disputes, such as fraud and theft, which may be addressed with digital evidence, not just information security defense against criminal hackers.	Organizations are not sure how to approach the legal entities when it comes to presenting a case in the court. Also organizations may not be confident about the nature of evidence to be presented.
An organization can be involved with all aspects of an investigation, not just the digital forensics.	Organizations worry about the “negative publicity” that might get generated and its impact on clients as well as organization’s brand image.
There are high costs associated with additional measures to prepare for digital forensics investigations compared with the potential benefits.	There is a perception in the organization that forensics is costly and may not yield the desired results even after spending the money. In general, investigations should be cost-effective and not just technically feasible.
Organization is not sure why much energy, time and cost should be spent in proactively gathering potential evidences.	In a corporate environment there is a wide range of potential evidence sources; digital evidence must be actively sought, not passively used.
In a corporate environment, staff members who configure and maintain audit logs may not be aware of the “high-level” crimes and business issues that can be detected with help of logs.	In most organizations, the security staff is <i>not</i> trained for forensics. In fact, their awareness about cybercrimes is low at most times.
To collect useful evidence, an organization needs to target its collection capability on the risks to the business; it is not a technical issue of what should be recorded in log files.	Collecting digital evidence is an activity in itself; when a disaster takes place, restoration is the first objective and not evidence collection, therefore the staff priorities differ.
Monitoring to detect an incident can encompass a wide range of techniques including CCTV, door swipes and honey pots. It is not just a case of applying an intrusion detection system (IDS).	IDS in itself is not the solution when it comes to cybercrime.
To collect admissible evidence, the organization needs to review the legality of any monitoring; it is not a technical issue of what can be “sniffed” or traced.	Legal awareness/overview to security staff helps.
When there is a requirement for evidence, all forms of potential evidence should be considered, such as CCTV cameras, personnel records, access control systems, etc. and not just log files and hard disks.	Evidence can be in multiple places and on multiple devices. Evidence can exist in multiple forms. It needs a forensically trained mind to “smell” evidence.
Staff may become involved in an investigation and will need to understand their roles; it is not just a job of the forensics investigator or system managers.	Forensics investigation is a collaborative process demanding team work.
When an incident takes place, the appropriate response must consider the options for forensics investigation and evidence preservation, and not just the immediate business continuity needs of containment, eradication and recovery.	There can be conflicts between incident response team and forensics expert because their objectives and priorities differ.
A major criminal incident may involve the police. Prior discussions with them can facilitate the interaction when an incident occurs.	It makes sense to have a legal department/legal advisor when costs justify their full-time presence. They serve as the interface between the organization and the police.

(Continued)

Table 9.6 | (Continued)

<i>Forensics-related Concern / Apprehensions</i>	<i>Remarks</i>
A major incident may become public knowledge and have reputation and brand image implications, therefore, company lawyers and media managers may be involved. It is not just an internal departmental issue.	The biggest fear is about the possible negative publicity; thus, corporate communication plays a vital role in such situations.
Corporate governance or regulatory enforcement often drives the preservation of digital evidence; it is not just due to an internal company issue.	Evidence involves ensuring the chain of custody and involves help from trained forensics experts.

1. Consider the nature of business, external drivers in the business environment and carry out systematic risk analysis. Review the results of the analysis and identify the business scenarios that require digital evidence.
2. Identify available sources of evidence and different types of potential evidence.
3. Determine the evidence collection requirement (technical as well as legal).
4. Establish a capability for secure gathering of legally admissible evidence to meet the requirement.
5. Establish a policy for secure storing and handling of potential evidence.
6. Ensure targeted monitoring to detect and deter major incidents.
7. Specify circumstances that warrant escalation for a full and formal investigation to be launched.
8. Train staff in incident awareness so that all those involved understand their role in the digital evidence process and also to make the staff appreciate legal sensitivities of evidence.
9. Be ready for evidence-based case documentation with an explanation about the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

A detailed guidance on these activities is provided in Part II of Appendix F (in CD).

9.10.4 Benefits of Being a Forensically Ready Organization

To conclude the discussion on forensics readiness, we present the benefits that an organization can derive from its forensics readiness:

1. The ability to gather evidence that can serve in the company's defense if subjected to a lawsuit.
2. Comprehensive evidence gathering can be developed as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cybercriminal).
3. In case of a major incident, a rapid and efficient investigation can be conducted and actions can be taken with a view to minimal disruption to the business.
4. Reduction in cost and time of an internal investigation through a systematic approach to evidence storage.
5. A structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g., in response to a request under data protection legislation).
6. Forensics readiness can widen the scope of information security to the wider threat from cybercrime, such as IP protection, fraud or extortion.

7. It demonstrates due diligence and good corporate governance of the company's information assets. It can further demonstrate that regulatory requirements have been met.
8. It can improve and facilitate the interface to law enforcement, if involved.
9. It can improve the prospects for a successful legal action.
10. It can provide evidence to resolve a commercial dispute.
11. It can support employee sanctions based on digital evidence (e.g., proving violation of an Acceptable Usage Policy).

Although the benefits look attractive, it should be noted that the costs of implementing forensics readiness may be significant, particularly in an organization with immature information security management processes. The regimentation that comes from the implementation of standards such as the ISO 27001, for example, does help in preparing grounds if organization plans to go for forensics readiness. Forensics readiness decision should be led by risk analysis exercise in the organization which may indicate that the nature of organizations makes them prone to frequent cyberattacks. Probably, it makes more sense for larger and multinational organizations to be forensically ready because their large and complex operations. Large client based would justify the costs involved in getting forensically ready. The costs are significantly ameliorated if the organization has already performed a comprehensive risk assessment, implemented a BCP and has programmed information security into staff training. In a more security-aware organization, forensics readiness can add value to many existing processes and leverage such activities as incident response, business continuity and crime prevention. Typically, costs are incurred in activities such as reviewing and updating policies, improvements in training, systematic gathering of potential evidence, secure storage of potential evidence, preparation for incidents, enhanced capability for evidence retrieval, legal advice and developing an in-house DFI capability, if required.

9.11 Media and Asset Protection: Best Practices for Organizations

The discussion in the previous sections is the background for appreciating the importance of media and asset protection. Organizations have their data/information stored on a number of media. Commonly used media in old days were floppy disks and they may exist even now though sparingly. Other media are – CD-ROM, DVD-ROM, hard disk, zip disk, jaz disk (similar to zip disk but may not be available anymore), backup tape, magneto-optical disk, digital audio tape (may still be used in some installations), flash drive, compact flash card, multimedia card, secure digital card, memory stick, smart media card, xD picture card, etc. Some of these media are shown in Figs. 7.6 and 7.7 in Chapter 7. Besides these, there are hidden and miniaturized storage media (see Fig. 7.2, Chapter 7 and Fig. 3.12, Chapter 3).



An “information asset” is a definable piece of information stored in any manner that is recognized as “valuable” to the organization.

Irrespective of the nature of the information assets themselves, they all have one or more of the following attributes:

1. They are recognized to be of value to the organization.
2. They cannot be easily replaced without incurring cost, skill, time, resources or a combination thereof.

3. They form a part of the organization's corporate identity (ID), without which the organization may be threatened.
 4. Their data classification would typically fall into three categories: (a) proprietary, (b) highly confidential or even (c) top secret.

Data breaches take place when criminals perceive “value” to the data/information stored on the media or see a particular information asset as valuable. All data breach incidents may not necessarily involve only network attacks; even physical media can get stolen and crimes happen. Remember the “BCBS Data Breach” mentioned in Section 9.1.2 – even when your critical data is stolen outright, legally you could be impacted if you cannot define your “critical data” and if you cannot prove that the data legitimately belongs to you. In today’s net-centric economy, information is the nerve system or the bloodline for organizations. Businesses take place in the global environment and networks are connected all the time. Almost all information assets exist in digital form and reside on corporate networks. Growth in employee mobility and remote working practices means that removable media may be used more often. Information assets can be compromised in many ways (see Fig. 9.19).

It is imperative to have local encryption for hard disks and any other media that are believed to store critical information. To begin with, there should be a scheme for information classification – it is the basic step in protection. One scheme is presented on the next page. Note however that information classification schemes vary from organization to organization.

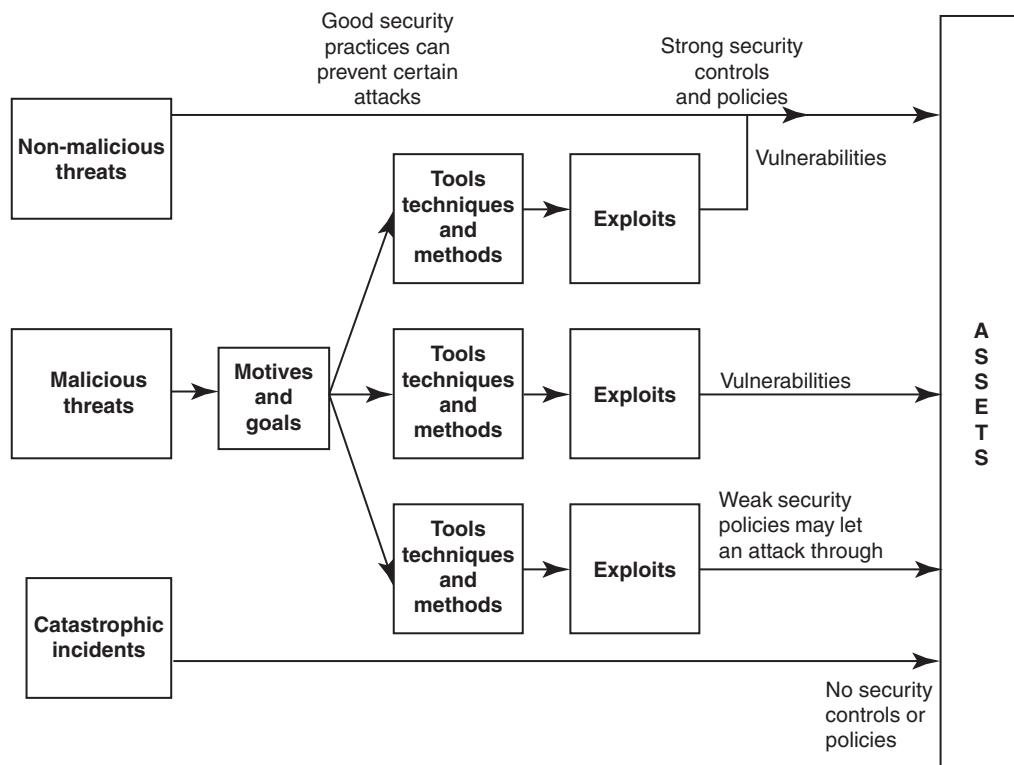


Figure 9.19 | The path to compromise an asset.

1. **Unclassified:** Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.
2. **Sensitive but unclassified (SBU):** Information that has been designated as a minor secret, but may not create serious damage if disclosed. Answers to questions in test papers are an example of this kind of information. Another example is healthcare information in a hospital database or information system.
3. **Confidential:** Information that is designated to be of a confidential nature. Unauthorized disclosure of this information could cause some damage to security. This level is used for documents labeled between SBU and Secret in terms of sensitivity.
4. **Secret:** Information that is designated to be of secret nature. Unauthorized disclosure of this information could result in serious damage to organization's security.
5. **Top secret:** This is the highest level of information classification (e.g., information in defense organizations). Unauthorized disclosure of top secret information will cause exceptionally grave damage to security.
6. **Public:** Information that is similar to unclassified information, that is, all information that does not fit into any of the other categories can be considered public. This information can be disclosed if required. Even if it is disclosed, it is not expected to seriously or adversely impact the company.
7. **Sensitive:** This type of information requires a higher level of classification than normal data. This information needs to be protected from a loss of confidentiality, as well as from a loss of integrity that may arise due to an unauthorized alteration.
8. **Private:** Typically, this information is considered of a personal nature and is intended for company internal use only. Its disclosure could adversely affect the company or its employees. Salary levels and medical information could be considered as examples of "private information." In HIPAA regulation, it is "PHI" – Protected Health Information.

Table 9.7 shows the key dimensions to be considered for setting priorities for protecting organization's information assets.

Table 9.7 | Information assets – the three key dimensions for protection prioritization

<i>The Dimension</i>	<i>Remarks</i>
Levels of INTEGRITY: These are defined to reflect the criticality of information assets and the impact of their unauthorized modification and the subsequent loss of accuracy.	<ol style="list-style-type: none"> 1. Basic integrity (routine) for normal purposes: This covers information where unauthorized damage or modification is not critical to business applications and business impact is minor. 2. Medium integrity: Where independent verification is required. This covers information where unauthorized damage or modification is not critical but noticeable to business applications and business impact is significant. 3. High integrity: This covers information where unauthorized damage or modification is highly critical to business applications and the business impact is major and could lead to serious or total failure of the business application, total shutdown of business operations or even closure of the business.
Levels of AVAILABILITY: These are defined to reflect the accessibility of information assets and the impact if such assets are not available within a specified timeframe as explained in the second column.	<ol style="list-style-type: none"> 1. Basic availability (routine): Information and services required for business applications and processes to be available within 12–48 hours.

(Continued)

Table 9.7 | (Continued)

<i>The Dimension</i>	<i>Remarks</i>
<p>Levels of CONFIDENTIALITY: These are defined to reflect the sensitivity of information assets and the impact of their unauthorized disclosure as explained in the second column.</p> <p><i>Note:</i> “Security” is C.I.A. (Confidentiality, Integrity and Availability – refer to Chapter 5, Ref. #1, Books, Further Reading).</p>	<ol style="list-style-type: none"> 2. Medium availability (priority): Information and services required for business applications and processes to be available within 12 hours. 3. High availability (high priority): Information and services required for business applications and processes to be available within 2–3 hours. 4. Very high availability (immediate): Information and services required for business applications and processes to be immediately available at all times. 1. Publicly available information: This refers to information that would cause no damage to the company if disclosed. This could be information that appears on the organization’s website, in marketing and sales promotion materials, public presentations and product user manuals. 2. “Internal use only” information: This refers to information available to any employee in the organization, but to which external access is granted only with authorization. The disclosure or loss of such information would be inappropriate and inconvenient, and could have an appreciable impact on the organization. This information is generally that which an organization simply wishes to keep private and it is likely to be of a routine, operational nature. It will constitute the largest category of information in most organizations. 3. “Confidential” information: This refers to information that is commercially sensitive and whose disclosure or loss would have a significant impact on the organization. For example, the impact might be financial or it might affect profitability, competitive advantage or business opportunities, or it might involve embarrassment or loss of reputation. 4. “Strictly confidential” information: This refers to information that is commercially sensitive and whose disclosure or loss would have a very significant impact on the organization. Again, the impact might be on the company’s finances or might affect its profits, competitive advantage or business opportunities, or involve embarrassment or loss of reputation; however, the loss or effect, whatever its nature, would be very serious. Organizations may also have information that is sector-specific and that may influence the levels of classification described above. One such type of information, held by many organizations, is “personal data/information” as indicated next. 5. “Personal data/information”: This covers information about employees, customers and other individuals that is protected by the Data Protection Act. Disclosure of such information could have serious legal consequences. Information falling into this category must be treated as “confidential” or “strictly confidential.”

Even when the information is classified and a scheme is deployed for information asset protection, it is of no use without an effective access management system. Managing the access to organization's information assets is of paramount importance. "Access" is the ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource. Access management is the process for managing individual and group authorization to read, create, modify or transfer data, and to perform specific functions or transactions. Access management framework is the consolidation of all access management standards, requirements and resource references to incorporate business unit best practices in a single document. Employees in the organization are committed to information protection and are responsible for classifying and protecting information that has value to the organization, its employees and the customers, suppliers, business partners and others with whom the organization does business, for example, the dimensions explained in Table 9.7 and in the fundamental privacy concepts (refer to Ref. #13, Books, Further Reading).

A well-architected access management framework in security-mature organization is guided by some governing principles that address information protection – classification and control of the organization's information assets. The following aspects are pivotal to a sound access management framework:

1. **What:** Identification of data and functions that need to be protected.
2. **Who:** Determination of who should have access to specific data and/or functions and why they should have access (authorization criteria).
3. **How:** Definition of the specific method to request, evaluate, approve (or reject) and implement access authorization.

Figure 9.20 presents the elements that affect an access management framework based on fundamental governance principles. The elements in the figure indicate that a mature access management framework spans across corporate instructions based on organizational standards and guidelines.

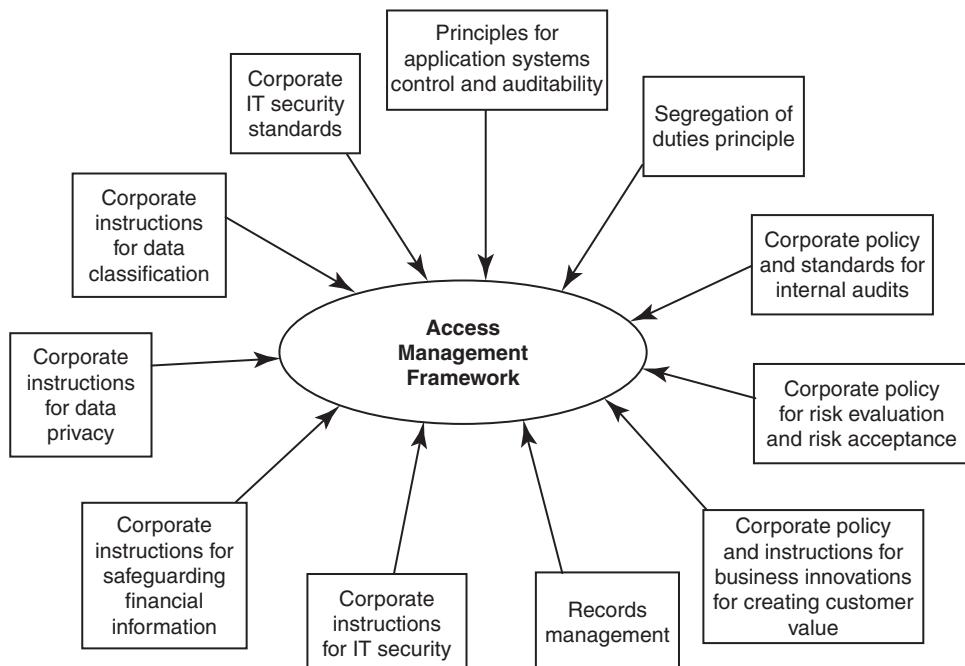


Figure 9.20 | Access management framework – key elements.

9.12 Importance of Endpoint Security in Organizations

Importance of media and asset protection is explained in the previous section. Insider attacks are on the rise as mentioned in the beginning of this chapter – that is why endpoint security becomes so important. People who are out of job are found to steal confidential company information with them either on DVD or using USB drives. Security risks from hand-held devices (such as iPods, USB devices, Smartphones, etc. – refer to Chapter 3) have dramatically increased the risk of intentional and unintentional data leaks and other malicious activity. An “endpoint” is an individual computer system or device that acts as a network client and serves as a workstation or personal computing device. Common endpoints are laptops, desktops and personal computing devices including hand-held devices that can connect into the network (refer to PDAs and many other devices mentioned in Chapter 3). The change in business paradigm in today’s global economy has created impact on the way people work and access data. Securing the endpoints is essential to protect assets. Organizations that do not have any form of endpoint security, have their corporate networks and data potentially exposed to hackers and criminals who can access sensitive information from unprotected access points.

Traditionally, the network perimeter was the first and primary line of defense from outside – untrusted networks and devices. It used to be the utmost point of contact for security defenses protecting the network and usually consisted of one or more firewalls and a set of strictly controlled servers located in a portion of the perimeter referred to as the DMZ. For networks relatively static and unchanging, the perimeter is the gateway to the outside world and, conversely, the outside world’s gateway to an organization’s network.

Today’s businesses’ demand real-time access to data spread across multiple sources – this has driven users to adapt and adopt the latest technologies. The use of portable storage devices poses a huge security risk to networks at the endpoints and securing these endpoints has become a major area of concern for IT security implementers in corporate as well as small and medium enterprises. Web-based applications are more prone to security threats. E-Mails have become the most common method or primary means of communication for almost all organizations and individuals. Most people are not careful when sending information through E-Mails. Refer to Box 2.7, Chapter 2.



Highly confidential information inside the E-Mail text and/or sent as attachments results in possible breach of confidential data through E-Mail system.

Although this practice is still a security risk in the client–server world, it is an even more dangerous activity in the webmail world.

Box 9.9 Be Careful with E-Mail and Attachments

When users access an E-Mail, it may have an attachment containing confidential information and typically, the mail may be from a third-party-owned computer. The user would choose either to “open” or “save” the document. In both cases, the file gets saved on the local hard drive and then a local application opens it as per user action. This document could be a business plan, customer information or revenue projections; in either case its confidentiality and integrity could be compromised if a Malicious Code resides on the local system; or more commonly, the document could be simply left in the local system’s temporary folder, on its desktop, or in its “My Documents” folder where the next person using the computer could view it. A simple search for “*.doc” or “*.xls” on a hotel business center, or other ample of public-use computer demonstrates how confidential documents are commonly left behind for anyone to steal. This type of search can be either very amusing or scary – it depends on whether you are the thief or the victim. Recall E-Mail-based attacks discussed in Box 2.7 and in Section 2.7 in Chapter 2.

Applications such as Web-based CRM and enterprise resource planning (ERP) are known to offer many benefits; however, due to the nature of these applications, they have a possible down side – they put sensitive information at risk. Customer information (top customers, revenues from top customer, etc.), sales forecasts, marketing strategy plans, project timelines, etc. are examples of information assets that organizations cannot afford to expose to their competitors and the public. Depending on the type of industry, failure to protect this information can result in regulatory violations (e.g., HIPAA – Health Insurance Portability and Accountability Act and its new security heightened by HITECH – Health Information Technology for Economic and Clinical Health Act, the GLBA – Graham-Leach-Bliley Act in USA, PCI-DSS for Financial and Banking Industry, PIPEDA – Personal Information Protection and Electronic Documents Act in Canada). With CRM applications, a sales team could store a sales forecast inside an Excel file on a computer. The moment that Excel file is downloaded, the enterprise loses control over it. For a greater understanding about regulatory compliance in information security domain, readers can refer to Ref. #5, Books, Further Reading.

Employees' access to corporate information is another area to focus on; organizational governance is essential for this – recall the discussion about access management (Section 9.11). Employees, depending on the roles they perform, have different corporate data usage profiles based upon their work patterns and job descriptions. “Workforce mobility” aspect provides an example worth considering – today's tele-workers access corporate information from home a majority of the time, while traveling workers access them primarily on the road, and day extenders and campus workers are at their desks most often when accessing corporate information. With various endpoints connecting remotely and internally at the same time, managing the endpoint infrastructure is an important – and challenging – task. All it takes is for one endpoint to become compromised to give attackers entry into your business network. From there, they can steal data, corrupt even more devices and possibly bring the entire network down. In addition, employees use a variety of corporate-owned and third-party-owned devices, such as laptops, workstations, kiosks, hotel business centers, customer and partner computers, to access the information.



Besides employees, in today's extended enterprise, there are many others who access corporate networks and the information residing on those networks.

Many third parties are involved in complex project delivery – for example, consultants, contractors, outsourcers, company agents and other partners often require some type of access to proprietary corporate information. Typically, organizations have little or no control over the endpoints connected to this corporate network. Despite the lack of control or weak control end-users with hand-held devices connected as endpoints into the corporate network may be given broad levels access to corporate resources.

Just antivirus installation and firewalls are not enough. Security of endpoint devices must be viewed from a network perspective. Endpoints must be prohibited from accessing the network until they meet the necessary security requirements. There are security solutions for the scenarios mentioned in the preceding paragraph. Most of the scenarios are integrated endpoint security solution for both corporate-owned and third-party-owned devices. These solutions are meant to protect corporate networks by preventing intrusions, enforcing security policies, and safeguarding confidential data. These solution enable enterprises to secure access methods, such as SSL VPN, webmail, Extranets and Intranets by ensuring the integrity of endpoints connecting to those portals and protecting the data that are transmitted to the endpoints. Endpoint security solutions test devices for compliance with the organization's security policy in the areas of antivirus, personal firewall, patches, security settings, and required and restricted software. They also ensure that worms, Trojans, viruses or Spyware have not compromised the device. Only those devices that meet the security

requirements are allowed access to the network and are also re-tested during their connection to ensure continued compliance.

Organizations can take a number of actions – first, devices can be tested for security compliance and devices that fail compliance testing should get quarantined. Second, users of those devices should be provided with direction and resources for updating the device with the necessary patches and security setting. It is to be remembered that endpoint compliance includes both kinds of devices:

1. Devices that are under the control of the organization (corporate desktops and laptops).
2. External endpoints that are not under the organization's direct control.

External endpoints include laptops and desktops that may be brought into the organization by visitors, contractors or employees and many other third-party entities depending on the situation. Over and above this, there are also devices that the organization may never physically “see”; for example, home-computers are used by employees and contractors for connecting into organization’s networks, as well as computing devices of all types (including mobile hand-held devices) that can connect to the corporate network via Wi-Fi – all these are also external/foreign endpoints. Although most IT organizations tend to focus their efforts on securing corporate-owned endpoints, external/foreign endpoints and corporate-owned devices may often get overlooked. They should also be included in the scope of organization’s endpoint security program. In fact, external/foreign endpoints pose much greater risk than corporate-owned machines – this is because their security compliance is not so known and likely to be inadequate or non-existent.



While addressing endpoint compliance, it is advisable to consider both external and internal perspective.

Testing of all external endpoints accessing the network should be made mandatory prior to granting them full access to organization’s network resources. A quarantine policy should be instituted whereby non-compliant devices should be provided only limited access, or may be even no network access until those devices meet endpoint security requirements. For example, the IT administrators may not allow people to update their home computers through the use of corporate VPN. The internal perspective involves controlling the access of the devices that connect directly to the internal local area network (LAN). Typically, this would include devices at a central location as well as devices at smaller or remote offices. Similar to external machines, these devices too should be segregated into a separate quarantine network with only the access necessary to receive virus definitions, update software or receive updates from a patch management solution.



Testing compliance endpoints involves more than checking for installation of latest patches and antivirus files.

Ideally, endpoint compliance requirements should include a wide range of security settings on the devices. Some examples of security requirements to be considered for endpoints as follows:

1. Updates to OS, hotfixes and critical updates;
2. automatic update settings for Windows;
3. installation of antivirus software and up-to-date virus definitions;
4. enabling personal firewall and up-to-date firewall rules;
5. installed software, programs or services;

6. registry entries;
7. banned software, including peer-to-peer and Spyware applications;
8. settings for application security, including use of “Macros”;
9. browser application, version and security settings;
10. local credentials stored – such as user IDs, passwords and .NET credentials.

There are hundreds of tools and products for securing the endpoint and improving its security health. This includes anti-malware programs, desktop firewalls, automatic patch updaters, an IDS, secure remote access tools and port lockdown (to prevent USB devices from connecting). Organizations need to ensure that all devices issued to employees are properly configured and that machines are locked down. Vulnerability scanners that scan all the machines within the enterprise enhance the risk management capabilities. However, they can address only the devices that are managed by the IT department. Residual risk remains with devices that are not managed by IT and devices that are more often on the road than in the office, that is, mobile workforce. Endpoint security touch points/check points are presented in Table 9.8. While useful, it is not an exhaustive list – it only addresses some common risks that organizations need to guard against.

Table 9.8 | Endpoint security – important touch points

<i>Endpoint Security Protection Element</i>	<i>Remarks</i>
Security policy: Establish security policy to identify and prioritize enterprise security requirements for periodic security audits.	Security audits cannot be done in a vacuum. Determine which information assets within your environment are proprietary and formulate a security policy for critical business processes that have access to this information. This policy document should form the basis for regular audits.
Secure logon mechanisms and strongly enforced password policies: There should be rules for password so that strong passwords are mandated <i>Note:</i> Recall the discussion in Section 4.4.3, Chapter 4 about “Strong, Weak and Random passwords.”	Use secure technologies for authentication; back it up with strictly enforced password policies. This will greatly strengthen the process of securing your environment.
Defining and deploying access policies on corporate firewall in sync with business requirements: Importance of access management is emphasized in Section 9.11.	There is a popular belief firewall that just installing one firewall fortifies the network. No firewall vendor would promise you such extraordinary simplicity. An out-of-the-box installation of the firewall, ignoring the specifics of your network, will not guarantee adequate protection. You need to configure it with appropriately designed access policies. Your business drivers in turn should articulate these policies.
Use of digital signatures for ensuring E-Mail confidentiality and use of encryption methods for enterprise messaging system: Although E-Mail systems received much focus, it should be kept in mind that messaging systems form the frontline for any organization. With the rise in the use of social media networking, messaging systems are getting highly used for corporate/business work.	Messaging systems are available today with digital signing and encryption capabilities. Most environments; however, do not implement these features. To fully leverage the functionality of E-Mail, it is vital that mail systems be configured to work with digital signing and encryption. The Indian IT Act has provisions on this.

(Continued)

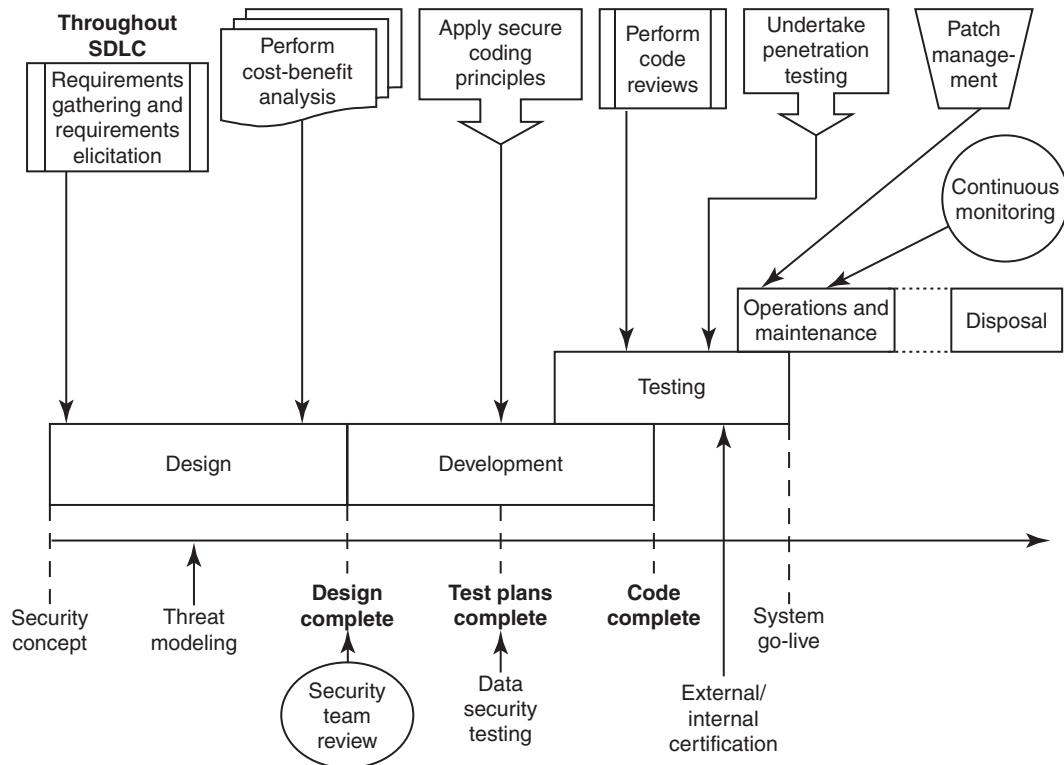
Table 9.8 | (Continued)

<i>Endpoint Security Protection Element</i>	<i>Remarks</i>
<p>Using certificates from a trusted authority on web servers that are used for implementing industry-standard protocols like SSL (Secure Sockets Layer), SET (secure electronic transaction) for server and client transactions. For technical discussion on these protocols, refer to Ref. #3, Books, Further Reading. Use systematic processes for hardening web servers, file and print servers and application servers.</p>	<p>Technologies such as Secure Sockets Layer (SSL), secure electronic transaction (SET) should be used for web server authentication, client authentication and channel encryption for securing transactions between your web servers and clients. Websites/servers should also be signed with digital certificates from a trusted authority, for example, VeriSign. As part of securing the network, mission critical servers should also be secured by closing unused ports, implementing IP-address-based restrictions, patching the system for known vulnerabilities, etc.</p>
<p>Guarding against Malicious Codes, Spam and viruses through strong defenses on Internet mail gateways.</p>	<p>Virus checking software should also be implemented at the mailbox level. It should be updated periodically to capture signatures of latest viruses.</p>
<p>Use of server audits to detect data security breaches.</p>	<p>Auditing on critical servers will help detect unauthorized access and facilitate incident handling mechanisms. It also dissuades users from trying to abuse the system when they know that their activity is being logged.</p>
<p>Monitoring systems to detect intrusion: IDS are useful for this. For greater details, refer to Ref. #2, Books, Further Reading.</p>	<p>The possible number of attacks on networks has been increasing consistently. IDS should enable the administrator to take manual or automated responses in real time against intrusions.</p>
<p>Systematic analysis of the logs generated in the organization: Tremendous learning about security weaknesses is possible through this exercise. When log files are analyzed, they point out access control weaknesses and its gaps. This exercise should be undertaken periodically, say quarterly or semiannually, depending on the size and complexity of the organization.</p>	<p>A system for the meaningful analysis of gigabyte-sized logs will play a key role in detecting anomalies in the network and reconnaissance scans from potential break-ins.</p>
<p>Incident handling mechanisms for security breaches: Refer to Section 9.9 for detailed discussion about incident response systems and the checklists mentioned in Section 9.9.8.</p>	<p>An information systems investigation procedure that addresses evidence preservation and forensics examination must be formulated with a trained response team in place to tackle the emergency.</p>
<p>Security controls on RAS (remote access server) to prevent unauthorized access through dial up lines: Workforce mobility is on the rise and security risks from remote access should not be overlooked.</p>	<p>To avoid any backdoor entries, the policies defined for RAS must be tightly coupled to the site security mechanisms, with emphasis on strong authentication schemes.</p>
<p>Guarded use of VPN for access to corporate Intranets: Virtual private network (VPN) creates a more secure communication channel. For detailed discussion on VPN and security, refer to Ref. #14, Books, Further Reading.</p>	<p>VPN technology allows corporations to connect branch offices or to connect to other companies over a public network, while maintaining secure communications.</p>
<p>Use appropriate security parameters on browsers and custom applications.</p>	<p>Browsers have several settings related to security, with each new release adding more options. Users usually do not modify the default settings, which add to the security risk in the environment. The same also applies to custom applications developed for the enterprise.</p>

(Continued)

Table 9.8 | (Continued)

<i>Endpoint Security Protection Element</i>	<i>Remarks</i>
Systematic and secure download distribution of trusted software: Recall discussion about “top security threats” Section 9.3.	To ensure reliable and trusted software downloads, it is a safe practice to download only signed software from certified websites. Similarly, it is advisable that all custom applications be signed before distributing to clients.
Sound software engineering practices to ensure development of secure custom applications: Secure coding practices to be encouraged. Sense of security needs to be inculcated throughout software development life cycle (SDLC) – see Fig. 9.21.	Adopting practices such as code reviews for security during the software development life cycle can prevent buffer overflows (refer to Section 4.11, Chapter 4). Efficient tools to check for buffer overflows also aid the cause of security.
Disaster recovery plan (DRP) against security breaches: Disasters and catastrophes can strike without warning! Best is to be prepared and have an organization-wide DRP strategy. For a detailed discussion on DRP and business continuity planning (BCP), refer to Ref. #9, Books, Further Reading.	The disaster recovery process should incorporate provisions for mirrored servers at a remote site, or even mirrored sites to ensure that denial-of-service attacks at one site do not lead to a meltdown of the network.

**Figure 9.21 |** Security throughout SDLC.

SUMMARY

In this chapter, we looked at a number of best practices in view of cybersecurity threats discussed in the previous chapters – asset and media protection, access management and endpoint protection. We also addressed cautions and care to be taken while using social media marketing and social computing. Organizational safe computing guidelines were also explained in detail along with incident response handling. Throughout the chapter, attention was drawn to regulatory considerations where applicable. With today's networked environment with computing devices connected through the Internet, such threats arising from infected non-genuine software have far reaching implications for an entire network.

The increasing use of social media has resulted in additional risks for corporate networks. There is no go without continuous employee awareness building, although it is only a preventive measure and is often limited in its ability to avoid new risks. With a proper security strategy that combines employee training with the newest technologies, organizations of all sizes can benefit from the advantages of social networking. At the same time, internal network protection mechanisms that

identify and terminate attacks in time are becoming more and more important. With the rise in workforce mobility, organizations cannot afford to overlook endpoint security. Taking a network perspective to endpoint security is a fundamental requirement for any organization to effectively defend itself.

For today's net-centric organizations operating in the global economy, information has become one of the most crucial assets of all the corporations. As more and more information gets stored in digital format, the onus is on us to guard the data and deliver business in a secure, reliable fashion. Our global clients expect assurance of data integrity, confidentiality and availability and it is our job to ensure that we honor the trust placed on us by our clients. In the face of cybersecurity challenges, appropriate controls must be maintained. One of the required corporate action for attaining this assurance is to ensure that unauthorized access, unauthorized use are prevented and disruptions in service is minimized. This makes it mandatory for organizations to ensure adequate level of server security and utility assessment so that it is used only for the right service and right purpose.

REVIEW QUESTIONS

1. What is a “security breach”? Explain the impact it has on an organization. Provide examples, either those mentioned in the chapter or your own examples from observations you may have made.
2. What are “PI” and “SPI”? Explain with appropriate examples.
3. What is meant by “insider threat”? How does it affect organizations?
4. Do you see a “pattern” in today’s cybersecurity threats? What are your comments on the sophistication of cybersecurity attacks? Do you see a “paradigm shift” with cybersecurity threats? Support your comment with examples.
5. Are “information security” and “cybersecurity” two independent domains? Explain your answer with examples to support your rationale.
6. What are the four dimensions of “privacy”? Do they all relate to data security? Justify your answer with suitable examples.
7. What are some of the key challenges to organizations as explained in this chapter? Describe them briefly in your words.
8. Are there costs associated with cybercrimes? What are the typical components of those costs? Do you see a “pattern” in those costs? Explain.
9. When it comes to forensics investigations, owing to its nature, there are certain aspects which often are exploited by cyberattackers/cybercriminals – what are those aspects as described in the chapter?

10. How does software piracy impact organizations? What care should be taken by organizations?
11. Prepare a short note on evils and perils of cyberthreats for organizations.
12. Can “cookies” impact data security and personal security? Explain how.
13. Describe any three of the “fair information practices” in the context of cookie usage in website design.
14. Should organizations monitor employees’ “Internet surfing”? Provide two arguments in favor of monitoring and two against it. Provide rationale for both sides of the argument.
15. What are some of the challenges brought by the rise in workforce mobility?
16. What is “cloud computing”? Is it completely safe? What are some of the challenges associated with cloud computing?
17. What do you think about use of social media marketing tools? What are some of the benefits and some of the associated threats? What care should organizations take?
18. Is “social computing” same as “social media marketing”? In what way are the two related if at all?
19. Explain “dataveillance” and “browse-fingerprinting.” Do these phenomena threaten our online privacy? How?
20. Can organizations really protect the privacy of people?
21. What are “anonymizers”? Are they a threat or a boon?
22. Explain how “safe computing guidelines” help when instituted appropriately by organizations.
23. Describe incident response life cycle along with the typical activities involved in each of the phases.
24. Explain with a suitable diagram how the three terms – *incident response*, *incident handling* and *incident management* are related.
25. Is “security management” same as “incident management”? Explain the differences and similarities, if any.
26. Prepare a short note on “organizational best practices for cybersecurity.”
27. What is meant by “forensics readiness?” Are there benefits for organizations when they have this readiness? How does incident response activity organization contribute to forensics readiness of an organization?
28. Why should organization’s media and information assets be protected?
29. What is an “endpoint” in a corporate network? Why is endpoint security important?
30. Describe any three key practices in organization’s endpoint security program.

REFERENCES

- [1] Below are the links to Nina Gogbole’s talk about *Workforce Mobility Challenges and Issues*. The first link below is about Nina Godbole’s talk on the topic of “*Working From Home: Myths and Truths*” and the second link is where you will find the copy of the article in PCQuest February 2010 issue.
<http://pcquest.ciol.com/content/techtrends/2010/110010806.asp> (7 August 2010).
<http://pcquest.ciol.com/content/topstories/2010/110020105.asp> (7 August 2020).
The pdf copy of Nina Godbole’s presentation at the PCQuest SummIT 2009 talk can be downloaded at:
<http://pcquest.ciol.com/infrasummit/2009/presentation/Nina-WorkForceMobility%5BDelegateCopy-PCQuest%20SummIT%202009%5D.pdf> (7 August 2010).
- [2] The following link on Top 5 Insider Attacks of 2009 is available at: <http://www.network-world.com/podcasts/panorama/2009/121609pan-insideattacks.html> (1 August 2010). There is an audio MP3 downloadable on this site.
- [3] Following are the links quoted for *Websense Tool* mentioned in Section 9.3 (Web Threats for Organizations: The Evils and Perils).

Features of Websense Enterprise Edition are described at: <http://www.securitybrigade.com/products/websense/enterprise.php> (12 September 2010).

To learn about *Websense Web Security Protection from Web-Based Threats*, visit:
<http://www.guardsense.com/Web-Security.asp> (13 September 2010).

Remote filtering features from Websense are described at:

<http://www.ciol.com/Ciol-Techportal/content/Security/News/2005/205091962.asp> (12 September 2010).

Read more about what is possible with Websense Remote Filtering Tool in the following URL:
<http://www.ciol.com/Ciol-Techportal/content/Security/Interviews/2006/2060620505.asp> (14 September 2010).

FURTHER READING

Additional Useful Web References

1. Five top cybersecurity risks are mentioned in the following link: <http://www.crn.com/news/security/220000395/five-top-cybersecurity-risks.htm> (8 October 2010).
2. In the following link, there is a posting titled “Obama Cybersecurity Report Addresses Critical Infrastructure and Privacy Issues”: <http://www.wired.com/threatlevel/2009/05/5638/> (8 October 2010).
3. *Cyber Security Threat to India is Real* – this article can be accessed at: <http://news.rediff.com/special/2009/aug/05/cyber-security-threat-to-india-is-real.htm> (8 October 2010).
4. “Cybersecurity in India: An Ignored World” – the article can be accessed at: <http://www.crime-research.org/articles/Cybersecurity-India-Ignored-World/> (8 October 2010).
5. Like the “Big Brother” syndrome, for a very interesting topic whether the Government can know what kind of websites you are visiting, you can visit: <http://computer.howstuffworks.com/government-see-website2.htm> (8 August 2010). In this link, on the middle, there is also a link to virus related video. You may run that at your own risk.
6. The *Top 10 Cyber Threats of 2009* are mentioned at: <http://www.aakashjain.com/misc/10-cyber-threats-to-look-for-in-2009-648> (1 August 2010). Those threats are (a) collaboration tools, (b) virtualization, (c) Botnet, (d) cyber warfare, (e) phlashing attacks, (f) wireless attacks, (g) threats due to green computing, (h) cloud computing, (i) insider threats, (j) risks for OS other than Windows.
7. In the following link, there is a *US Government Report* about the likelihood of extremists increasing cyberattacks: <http://www.fas.org/irp/eprint/leftwing.pdf> (8 August 2010).
8. How much of work hours are spent surfing by UK employees? Read some interesting information about this at: <http://www.cbi.org.uk/ndbs/Press.nsf/0363c1f07c6ca12a8025671c00381cc7/94d596bf6bcd69708025745e003b722b?OpenDocument> (9 August 2010).
9. Visit the following link for discussion blogs about “Social Media Security”: <http://socialmediasecurity.com/> (28 August 2010).
10. *2010 Social Media Marketing Benchmark Report* can be read at: http://www.marketingsherpa.com/SocialMedia_Marketing2010EXE.pdf (13 August 2010).
11. Following are links to some known companies that claim to provide *security solutions with the use of social media marketing*:
<http://www.stonesoft.com/en/> (29 August 2010). A Finland-based security solutions company.
Information about *Social Media Monitoring Tools* can be found at:
<http://www.toprankblog.com/2009/12/near-free-social-media-monitoring/> (29 August 2010).

12. *Social Media Marketing* – the following link can be used by those who are interested in reading the view of Rohit Bhargava about where social marketing media is heading. Rohit is a well-respected marketer and blogger and frequent speaker at conferences: <https://www.marketing-profs.com/login/join.asp?adref=rdblk&source=http%3A%2F%2Fwww%2Emarketingprofs%2Ecom%2F8%2Fgetting%2Dsocial%2Dwith%2Dsocial%2Dmedia%2Drohit%2Dbhargava%2Dcollier%2Easp> (31 August 2010).

13. In reference to Section 9.7 (Protecting People's Privacy in the Organization), some useful weblinks are as follows:

In the following link: read the interesting story about what Nandan Nilekani is up to with 8 gizmos in a case, to give 1.2 billion Indian people an identity!

http://in.news.yahoo.com/48/20100830/804/tnl-with-8-gizmos-in-a-case-nilekani-set_1.html (29 August 2010).

"People" is the difficult link in InfoSec Chain. Access the document *People is the Key Challenge in InfoSec* – NASSCOM survey to support the point at:

http://www.dsci.in/images/pdf/People%20the%20key%20challenge%20in%20info%20security_Survey.pdf (29 August 2010).

In the following link, there is a view point on whether the Unique Identification Authority of India (UIDAI) legally constituted:

<http://cyberlawsinindia.blogspot.com/2009/09/is-unique-identification-authority-of.html> (29 August 2010).

For *Unique Identification Authority of India*, the Wikipedia note is worth reading at:

http://en.wikipedia.org/wiki/Unique_Identification_Authority_of_India (29 August 2010).

Information about *Multipurpose National Identity Card* is available at:

http://en.wikipedia.org/wiki/Multipurpose_National_Identity_Card (29 August 2010).

14. In reference to Section 9.9 (Incident Handling: An Essential Component of Cybersecurity), following are some useful weblinks:

Handling a Security Incident – a useful paper can be accessed at:

http://www.qaiworldwide.org/pdf_files/aug08_pw.pdf (4 October 2010).

15. Following are some useful links for cybersecurity standards:

To know more on cybersecurity standards, visit: http://en.wikipedia.org/wiki/Cyber_security_standards (1 October 2010).

To know more on cybersecurity regulation, visit:

http://en.wikipedia.org/wiki/Cyber-security_regulation (1 October 2010).

To know more on Cybersecurity – WIKI, visit: <http://www.cybersecuritywiki.com/> (1 October 2010).

16. Following are some useful links about "anonymizers":

http://www.sonntag.cc/teaching/LTAEC_Budapest/Anonymizers/index.html (2 October 2010).

<http://en.wikipedia.org/wiki/Anonymizer> (2 October 2010).

http://www.livinginternet.com/i/is_anon_work.htm (2 October 2010).

http://www.livinginternet.com/i/is_anon.htm (2 October 2010).

<http://www.ucertify.com/article/what-are-anonymizers.html> (2 October 2010).

<http://www.guard-privacy-and-online-security.com/free-proxy-anonymizers.html> (2 October 2010).

17. A useful Wikipedia note about "proxy servers" is available at: http://en.wikipedia.org/wiki/Proxy_server (5 October 2010).

18. In reference to *Incident Management* discussion in Section 9.9 the *2009 Annual Report of Indian Computer Emergency Response Team India (CERT-In)* can be accessed at:

<http://www.cert-in.org.in/knowledgebase/annual-report/annualreport09.pdf> (3 October 2010).

To know about ITIL Incident Management for Beginners, visit: <http://www.slideshare.net/agnihotry/itil-incident-management-for-beginners> (18 November 2010).

Read about Benefits of Incident Management at: http://www.helpdesksurvival.com/Benefits_of_Incident-Management.html (18 November 2010).

Read about Incident Logging and Classification at: http://itil.osiatis.es/ITIL_course/it_service_management/incident_management/process_incident_management/incident_logging_and_classification.php (19 November 2010).

19. The *FISMA 2007 DRAFT about National Incident Management System* can be downloaded from the following link: <http://www.fema.gov/pdf/emergency/nrf/nrf-nims.pdf> (6 October 2010).

20. In the following link, there is a good article about *Incident Response Policies and Procedures*: http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1069767,00.html (4 October 2010).

21. *Security Standard: Computer Incident Handling Process* – A Plain English Guide providing explanation and illustration of this standard can be found at: <http://security.rit.edu/> (6 October 2010).

22. For Web 2.0 (mentioned in section 9.5.1) refer to the following links for additional information: <http://webdesign.about.com/od/web20/a/aa021306.htm> (What is Web 2.) (17 November 2010).

http://www.vinfotech.com/web_2.0/index.html (Web 2.0 Design and Development) (17 November 2010).

<http://www.dotnetuncle.com/Articles/Web-2-and-ASP-NET.aspx> (Web 2.0 and ASP.NET) (17 November 2010).

Video Clip to Web 2.0 Designing Tips (17 November 2010).

Books

- Godbole, N. (2009) *Information Systems Security: Management: Metrics, Frameworks and Best Practices*, Chapters 2, 3, 4, 5, 36, 37 and 38, Wiley India, New Delhi.

- Ibid, Chapter 14 (Intrusion Detection for Securing the Networks) and Chapter 15 (Firewalls for Network Protection).
- Ibid, Chapter 11 (Network Security in Perspective) and Chapter 12 (Networking and Digital Communication Fundamentals).
- Ibid, Chapter 31 (Privacy – Technological Impacts) – Section 31.2 (Privacy Implications of RFID Technology).
- Ibid Chapter 27 (Laws and Legal Frameworks for Information Security) – Section 27.16 Building Security into Software/SDLC).
- Ibid, Chapter 35 (Auditing for Security) – Section 35.9 (Technology-based Audits – Vulnerability Scanning and Penetration Testing).
- Ibid Chapter 37 (Asset Management) – Section Managing Access to Organization's Information Assets (under Section 37.10).
- Ibid Chapter 4 (Information Security Management in Organizations).
- Ibid Chapter 34 (Business Continuity and Disaster Recovery Planning).
- Ibid Chapter 21 (Security of Operating Systems) – Section 21.8 Patched Operating System.
- Ibid Chapter 37 (Asset Management) – Section 37.3 Security Aspects in IT Asset Management.
- Ibid Chapter 6 (Information Security Risk Analysis).
- Ibid Chapter 29 (Privacy – Fundamental Concepts and Principles).
- Ibid Chapter 16 (Virtual Private Networks for Security).
- T. Mather, S. Kumaraswamy and S. Latif (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly. To read the article, visit: <http://oreilly.com/catalog/9780596802769/> (1 July 2010).

Articles and Research Papers

- Nina Godbole's article based on the talk delivered at the PCQuest SummIT conference, December 2009 can be read at: [http://pcquest.ciol.com/infrasummit/2009/presentation/Nina-WorkForceMobility\[Delegate Copy-PCQuest%20SummIT%202009\].pdf](http://pcquest.ciol.com/infrasummit/2009/presentation/Nina-WorkForceMobility[Delegate Copy-PCQuest%20SummIT%202009].pdf) (1 July 2010).

2. The DSCI 2009 study on *State of Data Security and Privacy in the Indian Industry* can be accessed at: http://www.naavi.org/cl_editorial_10/data_security_survey_2009_report_final_30th_dec_2009.pdf (1 October 2010).
3. Vicky Shah's article about *Security Incident Handling and Dealing with Law Enforcement Agencies* can be read at: <http://searchsecurity.techtarget.in/tip/Security-incident-handling-and-dealing-with-law-enforcement-agencies> (3 October 2010).
4. In the following link you can find guidance on *Customizing the Handling of an Unauthorized Access Incident*: http://www.qaiworldwide.org/pdf_files/sept08_pw.pdf (8 October 2010).
5. United States Government Accounting Office (GAO) 2005 comprehensive report on *Emerging Cyber Security Threats and Issues* is available at the following link: <http://www.au.af.mil/au/awc/awcgate/gao/d05231.pdf> (8 October 2010).

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, C, D, F, H, L, M, T, U, V. These are provided in the companion CD.

Index

Symbols

- 11/26 attacks in Mumbai, 289
- 2.5G, 86
- 2009 survey of Data Security Council of India (DSCI), 512
- 2G, 86
- 3G. *See* Third Generation (3G)
- 3G mobile networks, 84, 86
- 3G Network Attacks
 - DDoS, 86
 - DoS, 86
 - Malwares, viruses, worms, 86
 - Overbilling attack, 86
 - Signaling-level attacks, 86
 - Spoofed PDP, 86
- 3G Network, 85–86, 107
- 802.11x Networking Standards, 173–175, 177

A

- Access management framework, 558
- Access management system, 558
- Access points (AP), 172
- Acquisition of digital evidence – legal and technical challenge, 329
- Active attacks, 49
 - tools, 54–58
- Active Server Pages (ASP), 167
- Active X, 146
- Address Resolution Protocol (ARP), 331
- Admissibility of digital evidence, 264
- Admissibility of electronic records, 265–268
 - amendments in the Indian IT Act, 264–269
- Advanced Encryption Standard (AES), 113, 175

- Advantage
 - of a computer forensics examination, 478
 - of P2P networks, 154
- “Advertisement information” transmitted over networks, 239
- Adware, 72, 75, 126, 152
- AES. *See* Advanced Encryption Standard
- Aggregated information, 236
- Aim of a forensics investigation, 476
- Alignment position
 - of Asia-Pacific countries with regard to Microsoft’s Model Privacy Bill, 237
 - of countries with regard to CoE’s Convention on Cybercrime, 235
- Amendments to the IT Act, 228
- Amendments, 319
 - to the IT Act, 228
 - Indian IT Act, 259
- ANA. *See* Internet Assigned Numbers Authority
- Analog Mobile Phone Service (AMPS), 426
- Analysis, interpretation and attribution of evidence, 347–351
- Android – Google, 84
- Anonymizer, 130
- Anti-Cybersquatting Consumer Protection Act, 579
- Antiforensics, 318, 406–408
 - methods, 369, 389
- Antkeylogger, 140
- Anti-Phishing plug-ins, 205
- Anti-Phishing Working Group (APWG), 186
- Anti-Spam Act, 244
- Anti-Spam legislation, 238
- Antispy, 140
- Anti-Spyware, 73, 140, 220
- Antistatic bags, 473
- Antivirus software, 68, 85, 120
- Antivirus, 72, 101, 140, 146, 154, 198, 220
- Anto. *See* Access points
- APEC Privacy Framework, 233–234, 238
 - 9 principles, 234
- API. *See* Application Program Interface
- Apple iPhone, 84, 445
- Application fraud, 88
- Application program interface (API), 91, 98
- APWG. *See* Anti-Phishing Working Group
- Asia-Pacific Economic Co-operation (APEC) Privacy Framework, 233
- ASP – Active Server Pages, 167
- Assurance and Compliance
 - security audits, 759, 767
 - types, 760–761
- Asymmetric warfare, 593
- Attacks
 - active, 49
 - mobile phones, 99–107
 - passive, 49, 65
 - through printer exploits, 441
 - vectors, 73–74, 79, 126
 - on wireless networks, 171–176
 - zero-day, 74
 - zero-hour, 74
- Audit of E-documents – Section 7A of Indian IT Act, 294
- Auditing vis-à-vis Cyberforensics Investigation, 404–405
- Australian Cybercrime Act 2001, 231–233
- Australian Legislation, 233
- Authentication, 133
- Authorization, 232
- Availability, 49
- Awareness about data privacy, 15

B

Backdoor, 128, 141, 195, 376
functions, 152–153
protection measures, 153–154
Bankers' Books Evidence Act, 264
Battery and memory storage
considerations – forensics
perspective, 484
BCM. *See* Business Continuity Management
BCMS. *See* Business Continuity Management System
BCP. *See* Business Continuity Plan
BellSouth Intelligent Wireless Network, 459
Binary rootkits, 370
Binning, 63
Biometrics, 115
Black hat, 47–48
Black hat SEO, 200
attacks, 200
Blackberry, 82
BlackBerry forensics
acquisition phase – care to be taken, 459
examination – evidence collection phase, 460
BlackBerry Serial Protocol, 459
Blended attacks, 539
Blended threat, 162, 539
Blind SQL injection, 165–166
tool, 166
Blocked ports, 61
Blue Screen of Death (BSOD), 161
Bluebugging, 106
Bluejacking, 106
Bluesnarfing, 106
Bluetooth, 83, 86, 100, 174
1.0, 105
2.0, 105
logo, 105
security issues, 106–107
Bluetooth – Hacking, 105–106
tools, 105
Boot sector viruses, 146
Borderless nature of cyberspace, 252
Bot, 71–72
Botnets, 14, 71–73, 79, 86, 141, 163, 187, 201

Brand Spoofing, 187
Breach of criminal law, 231
Breach of lawful contract, 302
Brown hat, 48
Browser
clear history, 69
settings, 69
temporary files, 69
Browser cookie, 130
Browser fingerprinting, 523
Brute force hacking, 46
BS 25999, 760
BSA and IDC Global Software Piracy Study, 28
BSI. *See* Business Sensitive Information
BSOD. *See* Blue Screen of Death
Bucket-brigade attack, 134
Buffer overflow, 126, 159, 168
attacks – prevention measures, 170–171
attacks – protection tools, 171
overrun, 98
types, 168–170
Buffer overrun, 168
Business Continuity Management (BCM), 760
Business Continuity Management System (BCMS), 760
Business Continuity Plan (BCP), 78, 551
Business identity theft, 212–213
countermeasures, 214–215
Business method patents, 577
Business Sensitive Information (BSI), 212
Bust-out, 212

C

Cache servers, 129
California Senate Bill 1386 384–385
Caller ID Spoofing, 103
Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), 243
Canadian Act for Protecting Personal Information, 243
CAN-SPAM Act, 188, 615
Car Whisperer, 106

Career paths in cybersecurity, 759–762
guide path, 767–771
Carpenter, 83
Cascading style sheets (CSS), 192
Categories – cybercrime, 48–49
CBK. *See* Common Body of Knowledge
CCK. *See* Complementary code keying
CD, 48
CDMA. *See* Code Division Multiple Access
CD-ROM, 110
Cell phone, 48, 89, 120
antitheft software, 100
attacks, 99–107
hardware and software features, 430–431
service provider, 99
theft (security tips), 99–100
working characteristics, 425–431
Cell seizure – forensics software toolkit, 466
Cellular networks, 84, 89
Cellular phone, 81
CERT. *See* Computer Emergency Response Team
CERT/CC. *See* Computer Emergency Response Team Coordination Center
Certifications, 762–767
vendor-neutral, 763
vendor-specific, 763
Certified ethical hacker, 582
C-Executives, 754
CGA. *See* Cryptographically Generated Addresses
CGI. *See* Common Gateway Interface
Chain of custody, 317, 325, 345, 388, 549
concept, 355–356
example, 326
purpose, 327
Chain of evidence, 368
concept, 356–357
Challenges
in the Asia-Pacific region, 231
in computer forensics, 389–395

- in digital evidence handling, 264
in forensics of the digital images and still camera, 454–458
to Indian Law and Cybercrime Scenario in India, 271–272
in iPhone forensics, 453
to law enforcement authorities, 479–480
“Channel Mixer” tool for image enhancement, 455
Characteristics of information hiding, 371
Checklists for handling incident response work, 548
Child identity theft, 217
Child online safety, 242
Child pornography, 16, 27, 48, 233, 241–242
Child prostitution and child pornography, 242
Children pornography – a global issue, 242
Children’s Online Privacy Protection Act (COPPA), 233
Chinese Ghost Net, 213
CIA Triad, 752
Class 1 misdemeanor, 230
Class 6 felony, 230
Class A misdemeanor, 229
Class B misdemeanor, 229
Class C felony, 229
Class D felony, 229
Classification
 cybersecurity certifications, 762–767
 DoS attack, 159
 password cracking attacks, 134–135
 social engineering, 62–65
 cybercrime, 228
Classified Information, 210
CLEW. *See* Closed-loop environment for wireless
Click forensics, 199
Click Fraud, 14, 197–199
Click throughs, 199
Clickjacking, 126
Closed ports, 61
Closed-loop environment for wireless (CLEW), 88
Cloud
 private, 76
 public, 76
 virtual private, 76
Cloud computing, 75–77
 advantages, 76
 and cybercrime, 77–79
 and cyberthreats, 515
 private cloud, 76
 public cloud, 76
 risk remediation, 78
 risks, 78
 service provider, 76, 78
 services, 77
 virtual private cloud, 76
Cloud service – characteristics, 75
Cloud, 75, 77
COBIT. *See* Control Objectives for Information Technology
Code Division Multiple Access (CDMA), 89, 426–427, 466
CoE Cyber Crime Convention, 37–38, 233, 247
COFEE. *See* Computer Online Forensics Evidence Extractor
Cognizable offense, 303
Collecting and recording digital evidence, 343–344
Collecting electronic evidence – precautions to take, 353–355
Commercial electronic message, 245
Commercial Wi-Fi hotspots, 174
Common Body of Knowledge (CBK), 767
Common Gateway Interface (CGI), 126
Common vulnerabilities – tools, 127
Communications and Multimedia Act of 1998, 237
Complementary code keying (CCK), 173
Compliance audits, 301
Compliance requirements
 in forensics field, 387
 of the EU (European Union) Data Protection Directive, 259
Compliers, 170
 tools, 170
Computer antiforensics, 369
Computer contaminant, 287
Computer crime, 12, 229
Computer Emergency Response Team (CERT), 69
Computer Emergency Response Team Coordination Center (CERT/CC), 163–164
Computer emulation software, 90
Computer Ethics, 583–584
Computer evidence, 324
 in the court – potential users, 478
Computer forensics, 317–318, 761–762, 769–771
 from compliance perspective, 383–389
compliance requirements – evidential implications, 388
definition, 320
expertise in India, 389
investigation, 358–361
methods and techniques, 324
 and OSI 7 Layer Model, 373–377
 and steganography, 368–373
Computer fraud, 12
Computer hacking and cracking, 229
Computer network intrusions, 30
Computer Online Forensics Evidence Extractor – COFEE, 320–321
Computer sabotage, 28–30
Computer safety, 233
Computer security
 and computer forensics, 318
 incident – defined, 531
 incident management, 537
Computer Security Incident Response Team (CSIRT), 253, 532
Computer security incident, 535
Computer Security Institute, 230
Computer security laws, 233–235
Computer trespassing, 230
Computer Usage Policy, 524–531
Computer virus hoax, 101
Computer viruses, 14, 45
Computer-based social engineering, 63–65
Computer-facilitated child pornography offenses, 241
Computer-related crime, 229
Conficker virus, 504
Confidentiality, 49

- Consequences of Not Addressing the Weakness in IT Act, 272–273
- Consumer protection laws, 240
- Content-injection Phishing, 199
- Contractual commitments, 300
- Contributors – Demand for IT Security, 754
- Control Objectives for Information Technology (COBIT), 760–761
- Control Panel setting, 93
- Convention on Cybercrime, 235
- Cookie, 131
- browser, 130
 - clues to forensics investigators, 443
 - DART, 130–131
 - Google, 130–131
 - HTTP, 130
 - and Internet Activities, 508
 - origin, 510
 - persistent, 130–131
 - and privacy concerns, 596
 - and privacy loss, 510–511
 - session, 130
- Copy protection vs. copyright protection – the difference, 575
- Copyright, 155, 574–576
- philosophy, 575
 - scope, 575
 - violation, 48
- Copyright Act, 504
- Corporate data usage profiles, 560
- Council of Europe's (CoE's) Convention on Cybercrime, 233
- Council of Europe's *Cyber Crime Treaty*, 36
- CPM. *See* Cryptographic Provider Manager
- Crack – password, 61
- Cracker tools, 46
- Cracker, 23, 45–46, 95, 592
- Cracking, 46
- Crash attack, 93
- Credit card frauds, 16, 31, 87, 589
- modern techniques, 90
 - prevention tips, 88
 - traditional techniques, 88–90
 - types and techniques, 88–90
- Credit card generators, 90
- Credit card machines, 89
- Credit card-related frauds, 250
- Crime under legal microscope, 230
- Crimes committed using computers, 253
- Crimes emanating from Usenet newsgroup, 18
- Crimes emanating from usenet newsgroup. *See* Newsgroup Spam
- “Crimes” in cyberspace, 572
- Criminal identity theft, 211–212
- Critical priority incidents, 537
- CRM. *See* Customer relationship management
- Cross-site request forgery (CSRF/XSRF), 192
- Cross-site scripting (XSS), 192
- Cryptographic checksums, 371
- Cryptographic Provider Manager (CPM), 94
- Cryptographic security, 93–94
- Cryptographically Generated Addresses (CGA), 93–94
- Cryptography, 91, 155–156
- security controls, 94
- CSRF. *See* Cross-site request forgery (CSRF/XSRF)
- CSS. *See* Cascading style sheets
- Current scenario
- on digital signatures under the Indian IT Act, 278–279
 - of threats prevailing in India, 304
- Customer relationship management (CRM), 113
- Cyber, 12
- Cyber espionage, 213
- Cyber Jihadist, 595–597
- Cyber jurisprudence, 309
- Cyber Law Compliance Audit, 293
- Cyberbullying, 67
- Cybercafe, 17, 67–71, 79
- and amendment to the Indian IT Act, 289–293
 - change password, 69
 - clear history, 69
 - and cybercrimes, 67–71
 - Internet banking, 70
 - password, 69
 - regulations, 289, 294
 - security, 70
 - temporary files, 69
- tough road ahead, 293
- virtual keyboard, 69–70
- Cybercrime
- against individual, 17
 - against property, 229
 - against society, 18
 - categories, 48–49
 - classification, 17–18
 - and cloud computing, 77–79
 - broad definition, 229, 232
 - definition, 1, 4, 36, 228–229
 - ethical dimension, 580–584
 - and extended enterprise, 38
 - and Federal Laws in US, 245–246
 - global perspective on, 36
 - and Indian ITA 2000, 34
 - Indian perspective, 32–34
 - and information security, 13–16, 306
 - investigation and litigation, 769
 - largest illegal industry, 227
 - laws in the Southern African region, 250
 - and legal landscape around the world, 230–253
 - legal perspective, 32
 - legislation, 250
 - legislation around the world, 305
 - legislation in African countries, 249–253
 - motives behind, 17
 - and other related crimes
 - punishable under Indian laws, 254
 - punishment, 305–307
 - statistics, 1
- Usenet Newsgroup as a source of, 30
- vis-à-vis traditional forms of crimes, 306
- worldwide-trends and patterns, 1
- Cyberdefamation, 19–21
- India's first case of, 21
- Cyberforensics, 317
- and digital evidence, 327–331
 - historical background of, 318–320
 - investigation delays, 294
- Cyberlaw, 227, 253
- Cyberlaw Advisory Group, 295

Cyberlaw and Technology – Indian Scenario, 307–309
 Cyberlaw compliance, 289, 319
 Cybernetics, 12
 Cyberoffences, 317
 Cyberpunks, 3, 571, 589
 Cybersecurity, 13, 287
 career paths, 759–762
 new legal definition, 282
 roles and responsibilities, 754–759
 Cybersecurity Certifications, 762
 classification, 762–767
 Cybersecurity implementation infrastructure in India, 288
 Cybersecurity incidents
 an ITIL perspective, 538–540
 risk levels, 534
 Cybersecurity infrastructure, 283
 Cybersociety, 21
 Cyberspace, 2
 Cybersquatting, 2, 574
 and trademarks, 579
 Cyberstalkers, 66–67
 offline stalkers, 66
 online stalkers, 66
 types, 66
 Cyberstalking, 16, 49, 79
 Cyberterrorism, 3, 18, 253, 501
 Cyberterrorists, 12, 571
 Cyberwarfare, 3

D

Damage to computers, 259
 DAP. *See* Directory Access Protocol
 Dark side cracker, 47
 DART cookie, 130–131
 DART search, 130
 Data breach offenses, 516
 Data Commissioner, 295, 303
 Data controller, 302
 Data diddling, 18, 21–22
 Data mining (DM), 113
 Data mining techniques, 389, 403
 used in Cyberforensics, 402–403
 Data privacy, 235–238
 issues in computer forensics, 392–395
 risks and cloud computing, 515

Data processor, 302
 Data protection, 231
 Directive, 247
 laws, 231
 legislation, 237
 and the New Clause 43A
 under the Amended IT Act, 259
 obligations, 303
 and privacy, 253
 Data reduction strategies, 390
 Data sanitization, 373
 Data subject, 301
 Data subject consent, 236
 Data theft, 13, 199
 Data vandalism, 295
 Data warehousing, 113
 Database vulnerabilities, 166
 Dataveillance, 523
 Daubert criteria, 470
 Daubert Hearing, 387
 Daubert Test, 387
 Daubert *v.* Merrell Dow Pharmaceuticals lawsuit, 470
 DDoS. *See* Distributed Denial of Service Attack
 Debates over privacy issues, 309
 Deceptive phishing, 196
 Defacement of websites, 499
 Defamatory E-Mails, 254
 Definitions
 for affixing of a digital signature, 278
 non-repudiation, 280
 Delivery of services by service providers – Section 6A of Indian IT Act, 294
 Demilitarized zone, 521
 Denial of Service (DoS) attack (DoS), 14, 18, 49, 71, 86, 93, 158–164, 589
 classification, 159
 detection tools, 164
 protection measures, 163
 tools, 161
 types, 160–161
 Device forensics, 431
 Device seizure, 432
 Device seizure, 464–465
 Dictionary attack measures, 238

Difference between forensics policy and security policy, 322–323
 live and dead analysis, 346
 physical evidence and digital evidence, 328
 steganography and cryptography, 156
 Digital Advanced Mobile Phone Service (D-AMPS), 428
 Digital camera – image acquisition
 Digital divide, 522
 Digital evidence, 227, 550–551
 admissibility in Courts, 263–264
 collection, 405
 and impact of business risks, 550
 sources, 330, 343
 vis-à-vis traditional evidence, 481
 Digital forensics, 317–318, 431–432
 definition, 320
 investigation, 550–551
 life cycle, 339–355
 phase-wise outputs, 353–354
 process, 339–341
 Digital forensics evidence (DFE), 325
 Digital Forensics Investigations and E-Discovery, 323–324
 Digital forensics science, 320–322
 an alternative definition, 318
 Digital forensics techniques – what they can do, 322
 Digital forensics tools ready reckoner, 397–399
 Digital Rights Management (DRM), 108, 576
 Digital signature
 and the Indian IT Act, 273–281
 in the ITA 2000, 274
 and public-key infrastructure technology, 276
 regulations, 279
 vis-à-vis traditional signature, 281
 Digital subscriber line (DSL), 173
 Digital warfare, 49
 Digital watermarking, 155, 576
 Direct sequence spread spectrum (DSSS), 173
 Directory Access Protocol (DAP), 95
 Directory Systems Agent (DSA), 96

- Disaster Recovery Plan (DRP), 78
Disclosure without consent, 302
Distributed Denial of Service Attack (DDoS), 72, 158–164
detection tools, 164
protection measures, 163
Distributed Phishing Attack (DPA), 201
DIY. *See* Do It Yourself
DLL. *See* Dynamic Link Library
DM. *See* Data mining
DNS – Domain Name Server, 219
DNS. *See* Domain name system
DNS hijacking, 197–199
DNS redirection, 198
DNS-based Phishing, 197
Do It Yourself (DIY), 201–202
DOCOMO – Do Communication Over the Mobile Network, 427
Documentary evidence, 329
DoD Data Sanitization Method, 373
Domain Name System (DNS), 96, 579
Domain name, 270, 579
Dragnet Phishing, 191
Drawbacks of P2P networks, 155
Drawbacks of peer-to-peer networks, 155
DRM. *See* Digital rights management
DRP. *See* Disaster Recovery Plan
DSA. *See* Directory Systems Agent
DSL. *See* Digital subscriber line
DSSS. *See* Direct sequence spread spectrum
Due diligence, 289
Dumpster diving, 63, 65, 134, 218
DVD player, 83
Dynamic IP address – non-PII, 237
Dynamic Link Library (DLL), 137
Dynamic ports, 59
Dynamic variables, 170
- E**
- Eavesdropping, 93, 106, 134, 174
E-Banks – Electronic banks, 121
E-Commerce. *See* Electronic Commerce
ECPA – Canadian Legislation, 244–245
E-crime. *See* Electronic Crime
EDI for Administration, Commerce and Transport – EDIFACT, 280
basics, 280
Efface online identity, 221
Effective fight against cybercrime – trio of important players, 309
Effective law enforcement, 306
E-Governance requirements, 293
Electronic banks (E-Banks), 121
Electronic Commerce (E-Commerce), 98, 108, 228, 253
Electronic Commerce Protection Act (ECPA), 243–244
Electronic Communications and Transactions Act (ECT Act), 252
Electronic Crime (E-crime), 126
Electronic evidence, 329
Electronic gadgets, 81
Electronic Messages and the Indian Evidence Act, 332–333
Electronic Signature, 277–278
E-Mail, 72
addresses – what they can reveal about their origin, 336
attachments, 65, 74–75
and attachments – care to be taken, 559
blockers, 188
bomb, 159
bombing/mail bombs, 18, 30
defamatory, 254
as evidence – points to remember, 334–335
fake, 64, 332, 336
header – how it looks, 336
header – how they are organized, 335
header information – forensic context, 333
Header Protocol Analysis – forensics, 333
hoax, 187, 190
junk, 187
server and E-Mail gateway, 332
spams, 18, 187, 190
Spoofing, 18, 186, 254
threatening, 254
tracing, 336
UBE, 187
UCE, 187
unique identifier, 337
unsolicited, 67
worms, 23
EnCase, 464
Encryption, 90, 111, 119–120, 133, 175
antiforensics technique, 389
key, 113
Endpoint
compliance requirements, 561
explained, 559
security – important points, 559–564
Enterprise Resource Planning (ERP), 153
Enterprise Risk Management (ERM), 757
Enumeration, 61
Equipment Identity Register (EIR), 433
ERM. *See* Enterprise Risk Management
ERP. *See* Enterprise Resource Planning
Ethical dimension of cybercrimes, 580–584
Ethical hackers, 48, 590–592
moral responsibilities, 581–582
Ethics and morality, 573, 581
E-Transactions Law, 237
EU Clause, 301
EU Contract Clause, 301–302
observations, 303
EU cybercrime law, 247
EU Data Protection Directive, 302
EU directive, 247
EU Legal Framework for Information Privacy to Prevent Cybercrime, 247–249
EU legal framework to prevent cybercrime, 231
EU member countries, 228, 247–248
EU's Data Protection Directive, 233
European Convention on Cybercrime, 250
European Convention on Human Rights (ECHR), 247

European Data Protection Directive, 248–249
 Event log of smartphone, 443
 Evidence preservation and investigation – key factors that matter, 551
 Evidence, 317
 Evidential integrity, 551
 Evidentiary copy of seized data, 364
 Evidentiary value, 320
 Examiner of electronic evidence, 295
 Examining/iInvestigating digital evidence, 346–347
Exchangeable Image File (EXIF), 219
 data, 219
 editors, 219
 Expert witness, 470, 477
 Exploitation tools, 588
 Extended enterprise, 38
Extensible Metadata Platform (XMP), 219
 External endpoints explained, 561
 External Ports, 60

F

Fair Information Practices (FIPs), 231
 Fake E-Mails, 64, 332
 creation tools, 336
 False claim of non-repudiation, 281
 Faraday bag, 429
 Federal Bureau of Investigation (FBI), 339
 view on digital evidence, 339
 Federal Rules of Evidence, 387
 Felony crimes, 230, 324
 FHSS. *See* Frequency hopping spread spectrum
 File carving – technique for digital forensics, 347–348
 File integrity scanners, 371
 File sharing, 75
 P2P networks, 75
 File Transfer Protocol (FTP), 60, 96, 153
 File-sharing programs, 73, 155
 Filter evasion Phishing, 193
 Financial fraud, 90

Financial identity theft, 211
 Financial losses
 due to cyberattacks, 230
 to the organization, 13
 Financial Privacy Rule – GLBA, 386
 FIR. *See* First Information Report
 Firewall, 73, 85, 97, 120, 140, 152, 173, 206, 220
 First Information Report (FIR), 68, 100, 433
 First-degree access, 229
 Flash Phishing, 193
 Flood attack, 160
 Florida Computer Crimes Act, 246
 Fly Fusion Pentop computer, 83
 Foistware, 75
 Footprinting, 50
 Forensic acquisition of media, 394
 Forensic analysis of cybercrimes, 332
 Forensic special tools and techniques, 396–403
 Forensic techniques, 317
 Forensically sound copy of hard drive, 387
 Forensics analysis of E-Mails, 332–339
 Forensics and Social Networking Sites, 377–383
 forensics auditing, 318, 403–404
 Forensics Card Reader, 466
 Forensics expert, 341
 benefits, 341
 Forensics from privacy perspective, 406
 Forensics investigation engagement contract – typical elements addressed, 359–360
 Forensics kits, 367
 Forensics of iPods and digital music devices, 467–474
 Forensics of the BlackBerry Wireless Device, 458–463
 Forensics policy
 guiding procedures, 551
 vs. security policy, 322–323
 Forensics procedures – its role in organization, 551
 Forensics readiness, 549
 defined, 548
 objectives, 551

Forensics science, 318
 Forensics validity issues about evidences, 479
 ForensicSIM, 467
 Forged (fake) E-Mail, 337
 Forgery, 18, 22
 Forum for Incident Response and Security Teams (FIRSTs), 253
 Fourth Amendment in the cyberspace, 395
 Fourth-degree access, 229
 Free proxy servers, 129
 Free Wi-Fi hotspots, 174
 Freeware, 73
 Frequency hopping spread spectrum (FHSS), 173
 FTP. *See* File Transfer Protocol
 Functions of Backdoor, 152–153

G

Gambling, 16
 Gathering information, 61
 GCC – GNU Compliance Connection, 170
 General Packet Radio Service (GPRS) Tunneling Protocol – GTP, 86
 General Packet Radio Service (GPRS), 86, 105, 116, 426
 Generations of hackers, 587
 Gen-Y, 108
 Geotagging, 219
 Getting forensically ready – key activities, 551–553
 Gillnet Phishing, 191
 GLBA. *See* Gramm-Leach Bliley Act
 Global Positioning System (GPS), 83, 430
 Global System for Mobile (GSM), 426, 466
 Global System for Mobile Communications (GSM), 89, 99, 107, 426
 Globally unique identifier, 339
 GNU Compliance Connection (GCC), 170
 Goal of professional ethics, 581
 Google – Android, 84
 Google cookie, 130–131

Google search
 allintitle, 51
 allinurl, 51
 being anonymous, 130
 cache, 51
 define, 51
 filetype, 50
 groups, 50
 info, 51
 intitle, 51
 inurl, 51
 link, 50
 related, 51
 site, 50
 stocks, 51
Googling, 50
Governance ambit of ECPA, 245
Government influence on information security industry, 303
GPRS. *See* General Packet Radio Service
GPS. *See* Global Positioning System
Graham-Leach-Bliley Act (GLBA), 259, 300, 385–386
 relevance to forensics, 386
Graphical User Interface (GUI), 106
Grey hat, 48
Grievance redressal mechanism, 303
Group policy, 93
GSM. *See* Global System for Mobile Communications
GTP. *See* General Packet Radio Service (GPRS) Tunneling Protocol
GUI. *See* Graphical User Interface
Guidelines for (digital) evidence collection phase, 330
Guidelines for Internet usage, 524–531
G-Zapper, 131

H

Hackers, 23, 46, 74, 107
 community, 585
 ethical, black hat, white hat,
 brown hat, grey hat, 48
 meaning of the term, 571
Hacking
 and Indian law(s), 34–35
 ITA 2008, 35–36
 motives behind, 23

Hacking, 45, 229
 tools, 128
Hacktivists, 571, 586
Hand-held devices, 82, 172, 431–432
Hard disk drive (HDD), 117
Hardware keylogger, 140
Hash functions, 133
Hashing, 347
Hats – black hat, white hat, brown hat, grey hat, 48
HDD. *See* Hard disk drive
Health Information Technology for Economic and Clinical Health Act (HITECH Act), 217, 300
Health Insurance Portability and Accountability Act (HIPAA), 78, 217, 259, 386
 definition of security incident, 386
 privacy rules, 386
Heap buffer overflow, 170
HIPAA. *See* Health Insurance Portability and Accountability Act
HIPAA-HITECH – Data Protection Implications for the Healthcare Industry, 300–301
HITECH. *See* Health Information Technology for Economic and Clinical Health Act
Hoax E-Mail, 187, 190
Hoaxbusters, 190
Hoaxes, 74
Home gateways, 98
Homograph Attack, 194
Host scans, 60
Hosts File Phishing, 197
HotSpot, 173
HTML. *See* Hyper Text Mark-up Language
HTTP. *See* Hypertext Transfer Protocol
Human Rights Commission, 305
Human-based social engineering, 62–63
Hybrid P2P, 154
Hyper Text Mark-up Language (HTML), 165
Hypertext Preprocessor (PHP), 201
Hypertext Transfer Protocol (HTTP), 60, 334
 cookie, 130

I

ICANN – Internet Corporation of Assigned Names and Numbers, 579
ICMEC – International Centre for Missing and Exploited Children (ICMEC), 241
ICMP – Internet Control Message Protocol, 160
ICMP – Internet Control Message Protocol, 161
ICMP – Internet Control Message Protocol, 60
ID theft. *See* Identity Theft (ID theft)
IDEN. *See* Integrated Digital Enhanced Network
Identifying digital evidence – contexts involved, 330
Identifying the evidence, 342–343
Identity cloning, 212
Identity theft (ID theft), 31–32, 65, 87, 90, 132, 185, 206–207, 228, 243
 computer-based techniques and consumer fraud, 385
 countermeasures, 220
 human-based methods, 218
 myths and facts, 208–209
 techniques, 218–219
 types, 211–217
Identity Theft Resource Center (ITRC), 206–207
IDN. *See* Internationalized Domain Name
IDS. *See* Intrusion detection systems
IEEE. *See* Institute of Electrical and Electronics Engineers
Illegal data flows, 302
Illicit IT jobs, 230
Image acquisition – digital camera, 457
Image forensics, 454
Images as evidence, 454
Imaging, 347, 429
IMEI. *See* International Mobile Equipment Identity
Impact
 of cyberforensics on legal practitioners, 394

- of oversights in Indian Act 2000 regarding digital signatures, 275–277
- Impersonation, 62, 95, 103
- Implications for Certifying Authorities, 277–278
- Importance of endpoint security, 559–564
- IMS. *See* IP Multimedia Subsystem
- Incident – SANS definition, 531
- Incident management system, 531 phases, 535
- Incident priority, 537
- Incident response procedures, 551
- Incident response systems, 545 benefits, 546–548 importance of, 537–538
- Incident response team, 545
- Incident response, 545
- Incidents – examples list, 534
- Incriminating evidence, 325
- India and Anti-Spam Legislation, 239–240
- India's Information Technology (Amendment) Bill 2006, 234
- India's Standing Committee on IT, 238
- Indian Citizens' right to protect their privacy, 295
- Indian Computer Emergency Team, 69, 293, 304
- Indian Copyright Act, 270
- Indian Evidence Act, 264 amended by Indian IT Act, 329 interpretations, 279
- Indian Information Technology Act (ITA) 2000, 68, 185, 206, 227–228, 254–270, 274–275, 318 in context of cybercrime, 228 cryptographic perspective, 279–281 digital signatures; current scenario, 278–279 liability regarding digital signature, 281 Section 6A – delivery of services by service providers, 294
- Indian IT companies and impact of IT Act Amendments, 295–296
- Indian online gambling market, 16
- Indian Penal Code (IPC), 19
- Indian perspective on cybercrime, 228
- Indian statistics on cybercrime, 230
- Indian website hacked, 1
- Indiscrete use of social networking sites, 377
- Industrial espionage, 18, 22, 45
- Industrial spy network, 213
- Industrial spying, 18, 22
- Information classified, 210 non-classified, 210
- Information and Communication Technology (ICT), 230, 573
- Information asset attributes, 554 what it is, 554
- Information assurance (IA), 751
- Information ethics, 583
- Information gathering, 79
- Information hiding, 371–373
- Information privacy, 231, 596
- Information security, 751 in India, 13 triad, 752
- Information Security Management System (ISMS), 760
- Information Technology Amendment Bill 2006, 277
- Information Technology Amendment Bill 2008, 277
- Information Technology Bill – the IT Act 2000, 254
- Information threats to organizations, 500
- Information Warfare Classification, 594
- Information Warfare, 593
- Infrared (IR), 100 ports, 120
- In-session Phishing, 196
- Insider attack examples, 498
- Insider threat – defined, 497
- Insider trading, 404
- Insider types, 497
- Insiders, 571
- Institute of Electrical and Electronics Engineers (IEEE), 173, 175
- Integrated Digital Enhanced Network (iDEN), 99
- Integrity and authenticity of digital images, 455
- Integrity of digital image, 454
- Integrity, 49
- Intellectual property, 253 crimes, 13 in cyberspace, 573–579 explained, 574
- Intermediaries, 286
- International Centre for Missing and Exploited Children (ICMEC), 233, 241 model child pornography legislation, 241
- International Mobile Equipment Identity (IMEI), 99, 433, 443
- International Mobile Subscriber Identity (IMSI), 443
- Internationalized Domain Name (IDN), 194
- Internet Assigned Numbers Authority, 60
- Internet banking, 70 virtual keyboard, 70
- Internet Control Message Protocol (ICMP), 60, 160–161
- Internet Corporation of Assigned Names and Numbers (ICANN), 579
- Internet Message Format, 338
- Internet phishing, 13
- Internet privacy, 596
- Internet Protocol address, 579
- Internet Protocol Security (IPSec), 94
- Internet Protocol version 6 (IPv6), 93
- Internet relay chat (IRC), 75, 161
- Internet safety, security and privacy legislation in the Asia-Pacific region, 231
- Internet Service Provider (ISP), 68, 73, 140, 188, 198
- Internet tablet, 83
- Internet time theft, 21
- Internet usage guidelines, 507
- Internet Users Association of India (IUAI), 289

Intrusion detection system (IDS), 120, 228
 Intrusion prevention system (IPS), 519
 Invalid E-Mail addresses, examples of, 338
 Investigating and prosecuting cybercrimes – technical and legal complexities, 306
 IP data security, 85
 IP Multimedia Subsystem (IMS), 86
 iPhone – Apple, 84
 iPhone forensics, 445–453
 iPhone Jailbroken Devices, 450
 iPhone worm, 450
 iPod features, 469–471
 iPod forensics
 legal considerations, 470
 techniques, 469–472
 IPSec – Internet Protocol Security, 94
 IPv6 – Internet Protocol version 6, 93
 IR. *See* Infrared (IR)
 IRC. *See* Internet relay chat
 ISMS. *See* Information Security Management System
 ISO/IEC 20000, 760
 ISO/IEC 27001, 760
 Isolation of potential evidence, 330
 ISP. *See* Internet Service Provider
 IT Act Amendments, 295
 impact on Indian IT companies, 295
 IT and ITES industries, 301
 IT Bill, 228
 IT evidence, 481
 IT governance framework, 760
 IT Security Organization, 754
 ITA 2000. *See* Indian Information Technology Act (ITA) 2000
 ITA 2008 (amendments to the Indian ITA 2000), 235
 and child pornography, 242
 and cybercafés, 290–292
 ITIL perspective on cybersecurity incidents, 538–540
 ITRC. *See* Identity Theft Resource Center

J

Jailbreaking, 450
 Jailbroken devices, 450
 Janus attack, 134
 Junk E-Mail, 187

K

Keylogger, 65, 68, 137–140, 195, 206
 phishing, 196
 Keylogging, 137

L

LAN. *See* Local area network
 Laptop theft, 117, 119
 Laptop, 48, 111, 120
 Laptops physical security, 117–120
 cables and hardwired locks, 117
 motion sensors and alarms, 117–119
 safes, 117
 warning labels and stamps, 119
 Law on defamation, 21
 Law on E-Transactions 2005, 234
 Laws for prevention of cybercrime, 243

LDAP. *See* Lightweight Directory Access Protocol
 Legal and regulatory frameworks, 231

Legal aspects of cybercrime, 227
 Legal challenges in computer forensics, 392–395

Legal drawbacks with regard to cybercrimes addressed in India, 271
 Legal governance, 231
 Legal infrastructure for E-Commerce in India, 253

Legal issues involved in cyberforensics, 318
 Legal principle of vicarious liability, 286

Legal side of cybercrime, 318
 Legal use and crypto-technical use of “non-repudiation” – distinction, 281

Legislative analysis in the Asia-Pacific region, 231
 Legislative position in Asia-Pacific countries – data privacy, 233

Levels of peer-to-peer (P2P) networking, 154
 Libel vs. slander, 21
 Libsafe, 171
 Lightweight Directory Access Protocol (LDAP), 91, 94–95
 directory structure, 96
 security, 94–95
 Limitations in the ITA 2000, 254

Linux viruses, 147
 Lobsterpot phishing, 191
 Local Area Network (LAN), 97, 116, 174

Locard, Dr. Edmond, 328
 Locard’s exchange principle, 328
 Log management, 388
 Logic bomb, 18
 Logical acquisition, 440
 Logical analysis of Smartphone data, 444
 Logs of IT activity, 388
 Losses to US Corporations due to spamming, 239
 Lottery frauds, 27

M

MAC. *See* Media access control
 MACRO, 146
 Macros, 75, 337, 562
 Macroviruses, 146
 Mail server software, 332
 Malicious Code, 14
 Malicious online activity, 231
 Malvertising, 126
 Malware incidents, 539
 Malware, 68, 72, 74, 86, 93, 100, 126, 141, 145, 194–195, 198, 200, 202
 Malware-based phishing, 196
 Man-in-the-middle attack (MITM), 93, 134
 Man-in-the-middle phishing, 199–200
 Masquerading, 95
 Mass Dataveillance, 523
 Master Boot Record (MBR), 146
 M-Banking. *See* Mobile banking
 MBR. *See* Master Boot Record
 M-Commerce. *See* Mobile commerce

- MCQ. *See* Multiple Choice Questions
- MDSR. *See* Multi-Dimensional Space Rotation
- Meaning of source code, 284
- Measures toward data protection, 295
- Media access control (MAC), 93, 175
- Media files, 98
- Media player, 91
 security, 98
- Medical identity theft, 215–217
- Members of the African Union, 250
- Memory stick, 108
- Merrell Dow Pharmaceuticals case, 470
- Message headers – importance for E-Mail message investigation, 332
- Message Transfer Agents (MTA), 335
- Message-ID field, 337
- MessageLabs Security SafeGuard tool, 509
- Microsoft ActiveSync, 92
- Microsoft exchange server, 92
- Microsoft Office, 92
- Microsoft Outlook, 92
- Microsoft-drafted Model Privacy Bill, 235
- MIMO – multiple-input–multiple-output, 173
- Mindset of hackers, 588
- Minimize buffer overflow attacks, 170–171
- Mishing, 101
- MITM. *See* Man-in-the-middle attack (MITM)
- Mixed P2P, 154
- MMS, 100
- Mobile and wireless devices
 organizational security measures, 112–114
 outbreaks, 100
 proliferation, 82–84
 trends, 84–86
- Mobile banking (M-Banking), 87, 108
- Mobile commerce (M-Commerce), 87, 98, 101
- Mobile computing, 82–84
 devices – organizational security policies, 114–116
- network security, 93
 security, 85, 93
- Mobile credit card transactions, 87
- Mobile device, 82, 93–94, 100, 111, 114–115, 121
 lost and stolen, 110–111
- RAS Security, 95–97
- registry settings, 92–93
- security challenges, 91–92
- security implications for organizations, 107–112
- threats through lost and stolen devices, 110–111
- TrustZone technology, 108
- Mobile Devices security
 macrochallenges, 91
 microchallenges, 91
- Mobile handsets, 81
 challenges, 428–429
 security and privacy risks associated, 425
- Mobile network, 85
- Mobile OS
 Symbian, 86
 Windows CE, 86
- Mobile phone
 antitheft software, 100
 hacking, 107
 theft (security tips), 99–100
- Mobile phone data acquisition – goal, 482
- Mobile phone evidence guidelines, 482–483
- Mobile phone forensics, 433–438
- Mobile phone virus hoax, 101
- Mobile phones, 81
 attacks, 99–107
- Mobile Security Processing System (MOSES), 86
- Mobile theft, 99
 insurance, 99
- Mobile virus, 101
- Mobile workers – type, 172
- Mobile workforce, 98
- MOBILedit, 466–467
- Mobility protocols, 94
- Mobitex Network, 89
- Model Privacy Bill, 237
- Model UNCITRAL law for E-Commerce, 254
- Modems, 173
- MOSES. *See* Mobile Security Processing System
- Motent Network, 89
- MP3 player, 83, 110
- MSDN, 98
- MTA. *See* Message Transfer Agents
- MtE. *See* Mutation Engine
- Multi-Dimensional Space Rotation (MDSR), 113
- Multipartite viruses, 146
- Multiple Choice Questions (MCQs), 767
- Multiple-input–multiple-output (MIMO), 173
- Music files, 98, 112
- Music gateway, 98
- Mutation Engine (MtE), 146
- ## N
- NASSCOM, 39, 259, 754
- National Institute of Standards and Technology (NIST), 385, 541
- NEED. *See* Network-enabled-embedded devices
- Need for Computer Forensics, 323–327
- Neo Hackers, 586
- Netizen Rights Commission, 293, 305
- Netizen's Rights Advisory Board, 305
- Network
 attack, 125
 vulnerabilities, 47
- Network-enabled-embedded devices, 162
- Network forensics, 357–358
 challenges, 390
- Network interface card (NIC), 175
- Network intrusions, 45
- Network security, 761, 768
- Network service providers in cybercafe context, 289
- Network sniffing, 51
- Network traffic, 51
- Network-enabled-embedded devices (NEED), 162
- Networking API Security, 98
- Networking Standards (802.11x), 173–175, 177

New Section 3A to define electronic signatures, 277
 Newbies, 571
 Newsgroup Spam, 22
 NIC – network interface card, 175
 NIST. *See* National Institute of Standards and Technology
 No Operation Performed (NOOP), 169
 No Operation Performed (NOP), 169
 Nodal agency, 304
 Non-classified Information, 210
 Non-repudiation, 279
 crypto-technical meaning, 281
 definitions, 280
 Non-uniform treatment of crimes across the world, 306
 NOOP. *See* No Operation/No Operation Performed
 NOP. *See* No Operation/No Operation Performed
 Nuke, 161
 Null bytes, 169

O

Observations
 EU Contract Clause, 303
 Section 43A of Indian IT Act, 300–301
 Section 67C of Indian IT Act, 303–304
 Section 72A of Indian IT Act, 302–303
 Sections 69A and 69B of Indian IT Act, 304–305
 ODBC. *See* Open Data Base Connectivity
 OFDM. *See* Orthogonal frequency division multiplexing
 Offline Cyberstalkers, 66
 Online anonymity, 247
 Online child safety laws, 233, 241–242
 Online cyberstalkers, 66
 Online frauds, 23–27
 Online gambling in India— legal status of, 16
 Online grooming, 522

Online privacy, 522, 596
 Online Protection for Children, 241–243
 Open Data Base Connectivity (ODBC), 168
 Open ports, 61
 Open-source software (OSS), 337
 Opt-Out anti-Spam regime, 238
 Oral admissions as to the contents of electronic records, 264
 Oral evidence, 329
 Organization for Economic Co-operation and Development (OECD), 237
 Organizational implications of software piracy, 504–505
 Organizational security policies – mobile computing devices, 114–116
 Orthogonal frequency division multiplexing (OFDM), 173
 OSI 7 Layer Model and computer forensics, 373–377
 Outsourcing to India, 259
 Overview of changes
 of cybercrime legislations, 228
 to Indian IT Act, 283–288
 Ownership of the patent, 578
 Oxygen Forensic Suite 2010, 467
 Oxygen Forensic Suite, 444

P

P2P file-sharing networks, 75
 P2P network, 153–155
 P2P networking – levels, 154
 P2P networks, 75
 drawbacks, 155
 PaaS. *See* Platform-as-a-service cloud computing
 Paper evidence vis-à-vis computer evidence, 477
 Paraben's device seizure, 447–448, 464
 Paradigm of cybersecurity, 228
 Passive attack, 49, 65
 tools, 52–53
 Password cracking, 61
 non-electronic attacks, 134
 offline attacks, 134
 online attacks, 134
 tools, 133–134
 types, 134–135
 Password policy guidelines, 136
 Password sniffing, 18, 30–31, 45
 Passwords, 65
 Patent
 explained, 576
 what it means, 577
 Patriot hacking, 49
 Payload, 74–75, 126, 158, 162, 169, 192
 Payment Card Industry Data Security Standard (PCI DSS), 78, 300
 Payment gateways, 98
 PayPal, 174
 PCI DSS. *See* Payment Card Industry Data Security Standard
 PCMCIA. *See* Personal Computer Memory Card International Association
 PDA. *See* Personal Digital Assistance
 PDoS attack. *See* Permanent Denial-of-Service (PDoS) attack
 PDP. *See* Policy Development Process
 Peculiar nature of cybercrime/ computer crime, 305
 Pedophiles – how they lure kids, 27
 Peer-to-peer network, 153–155
 drawbacks, 155
 Peer-to-peer networking – levels, 154
 Pen drive, 48
 Penalty for breach of confidentiality and privacy, 259
 Penalty for use of malicious Spyware, 246
 Pending computer security laws in India, 239
 Penetration testing, 54
 Permanent Denial-of-Service (PDoS) attack, 162
 Persistent cookie, 130–131
 Personal Computer Memory Card International Association (PCMCIA), 117, 173
 Personal Data Protection Act 2006, 295
 Personal data, 301
 Personal Dataveillance, 523

- Personal Digital Assistance (PDA), 48, 81–82, 84, 86, 105, 111, 113, 120–121, 136, 172
forensics, 438–440
seizure, 464–465
- Personal Identification Number (PIN), 88, 218, 220
- Personal information (PI), 13, 66, 75, 104, 231
defined, 496
- Personal Information Manager (PIM), 121
- Personally identifiable information (PII), 88, 91, 99, 209–210, 235, 751
definition, 236
- Pharming, 13, 197–198, 218
- Phases
computer forensics/digital forensics, 341–353
in incident management system, 535
- PHI. *See* Protected Health Information
- Phisher – Methods, 191
- Phishing, 13, 64, 90, 101, 131–132, 185, 218
countermeasures, 202–206
definitions, 187
how it works, 131–132
scams – types, 196–201
tactics, 189
techniques, 193–195
toolkits, 201–202
vis-à-vis spoofing, 192
- Phishing attacks, 249
SPS Algorithm, 204–206
- Phone phishing, 193
- Phoraging, 198
- PHP – Hypertext Preprocessor, 201
- Phrackers, 23
- Phreaking, 46
- Physical acquisition, 440
- Physical evidence vs. digital evidence – the difference, 328
- PI. *See* Personal Information
- PII. *See* Personally Identifiable Information
- PIM. *See* Personal Information Manager
- PIN. *See* Personal Identification Number
- Ping flood, 160
- Ping of death attack, 160
- Ping sweep, 126
- PIPEDA – Canada's Personal Information Protection and Electronic Documents Act, 243
- PIPEDA – FIPs (Fair Information Practices), 243
- Pirated software, 68
why employees use them, 504
- PKI. *See* Public-key infrastructure (PKI)
- Platform-as-a-service (PaaS) cloud computing, 77
- Pocket-sized devices, 84
- Point of Sale (POS), 87
- Policy Development Process (PDP), 86
- Policy for forensics, 550
- Policy Usage in the Organization, 509–510
- Political activists, 571
- Polymorphic generators, 146
- Polymorphic viruses, 146
- Polymorphism, 146
- Pop-up Window, 65, 73
- Pornographic offences, 27–28
- Pornography, 104
- Port numbers, 59
- Port scanning, 58, 60, 96–97, 126
- Port, 58–61
blocked, 61
closed, 61
externals, 60
infrared, 120
open, 61
USB, 110
well-known, registered, dynamic, private, 59–60
- Portable computer, 83
- Portsweep, 60
- POS. *See* Point of Sale
- Positive Aspects of the ITA 2000, 269
- Powers granted by Australian Cybercrime Act, 232–233
- Powers of interception and decryption, 304
- PR. *See* Public relations
- Preamble to the Indian ITA 2000, 253
- Preserving digital evidence from iPod, 473
- Preserving information as evidence for cyberoffenses, 286
- Pretexting, 103–104
- Prevent SQL injection attacks, 167
- Prevention Measures – Spear Phishing, 196
- Principles for information management, 247
- Printer forensics, 440–441
- Privacy, 573
best practices, 511
concerns with cookies, 596
key dimensions, 499
laws and Spam, 233
notice, 235
policy, 236, 510
regulations, 235
statement, 236
threats from social media marketing, 512–513
- Private cloud, 76
- Private ports, 59
- Proactive vs. Reactive Approach to Security, 512
- Processing of personal data within the EU, 247
- Processing personal information, 302
- Program viruses, 146
- Proliferation – Mobile and wireless devices, 82–84
- Protected Health Information (PHI), 65, 216–217
- Protecting online privacy, 523
- Protecting organization's information assets – key dimensions, 556–557
- Protection measures
geotagging, 219
Trojan Horses and backdoors, 153–154
- Protocol
Directory Access Protocol (DAP), 95
File Transfer Protocol (FTP), 60, 153
HTTP, 60
ICMP, 60, 160–161
SMTP, 60
TCP, 58, 60, 160

Protocol (*Continued*)

- TCP/IP, 58, 161
- Telnet, 60
- UDP, 58
- Voice over Internet Protocol (VoIP), 86, 93, 102
- Proxy server, 129–130, 206
 - purposes, 129
- Public cloud, 76
- Public relations (PR), 114
- Public-key certificates, 273
- Public-key infrastructure (PKI), 94
 - basic components, 276
 - public-key infrastructure, 94
 - risks, 281
- Pull attack, 93
- Pure P2P, 154
- Push attack, 93

Q

Quarantine policy, 561

R

- RAID. *See* Redundant Array of Independent (or inexpensive) Disks
- Ransomware, 126
- RAS. *See* Remote access server
- RDBMS. *See* Relational Database Management Systems
- Ready reckoner of forensics tools, 397–399
- Real life use of forensics, 474–475
- Real-time electronic surveillance, 394
- Reasonable security practices, 259, 294, 300
- Reasons for enactment of cyberlaws in India, 253
- Reasons why organizations use social media marketing, 517–518
- Recognize Legitimate Websites, 204
- Reconnaissance (information gathering), 49–50, 125, 128, 588
- Red teaming, 590
- Redundant Array of Independent (or inexpensive) Disks (RAID), 350–351
 - levels, 350–351

Redundant bits, 156

- Registered ports, 59
- Registration of data processors, 303
- Registry hacks, 93
- Registry settings, 91, 98
- Regulations for digital signatures, 279
- Regulatory perspective for forensics, 384–388
- Relational Database Management Systems (RDBMS), 164
- Remote access server (RAS), 47, 91, 95–97
 - system security, 97
- Removable medias (CDs, pen drives), 48
- Research in motion (RIM), 82, 458
- Reserve Bank of India Act, 264
- Restricted data, 232
- Return address, 171
- RFC2822 – Internet message format, 338–339
- Right to privacy, 247
- Rights of Netizens, 39
- RIM. *See* Research in Motion
- Risks
 - associated with geotagging, 219
 - of being negligent, 301
 - involved in PKI, 281
 - levels – cybersecurity incidents, 534
- Rod-and-reel Phishing, 191
- Rogue software, 126
- Role of computer forensics in litigations, 476–479
- Role of digital forensics, 321
- Root access, 126
- Rootkits, 141, 145, 369–370
 - classification, 370
 - important functions served, 370
- Routers, 173
- Rules of evidence, 329–331, 405, 481

S

- SaaS. *See* Software-as-a-service cloud computing
- Safe computing guidelines, 507, 524–531
- Safeguards Rule – GLBA, 386

Salami attack/Salami technique, 18, 21

- Sanitizing Proxy System (SPS), 204–206
 - characteristics, 206
- SANS definition of incident, 531
- Sarbanes Oxley Act (SOX), 78, 385
- Scanner forensics, 442
- Scanning, 61
 - scrutinizing, 58–61
- Scareware, 126
- Scavenging, 63
- Scenarios – forensic investigation, 321
- Script kiddie, 571, 587, 592
- Scrutinizing, 61
- Search – Google, 50
- Search engine marketing (SEM), 200
- Search engine optimization (SEO), 200
 - attacks, 200–201
- Search engine phishing, 200
- Search engine spamming, 19
- Search engine, 130
- Search warrant, 394
- Second-degree access, 229
- Section 66A (Offensive Messages), 282
- Section 66B (Receiving Stolen Computer), 282
- Section 66C (Identity Theft), 282
- Section 66D (Impersonation), 282
- Section 66E (Violation of Privacy), 282
- Section 66F (Cyber Terrorism), 282
- Section 67A (Sexually Explicit Content), 282
- Section 67B (Child Pornography), 282
- Section 7A – audit of E-documents, 294
- Secure coding, 307
- Secure electronic transactions (SET), 273
- Security – mobile computing, 85
- Security and privacy risks associated with use of mobile handsets, 425
- Security audit – compliance and assurance, 759
- Security breach, 237

- defined, 496
Security challenges – mobile devices, 91–92
Security fix, 74
Security policy, 510
 vs. forensics policy, 322–323
Security Processing Engine (SPE), 86
Self-splitting files, 371
SEM. *See* Search engine marketing
Sensitive information, 13
Sensitive personal data, 259
Sensitive personal information, 294–295, 300
SEO. *See* Search engine optimization
Service Level Agreements (SLAs), 300
Service marks, 577
Service provider – cloud computing, 78
Service set identifier (SSID), 174–175, 177, 179
Session cookie, 130
Session hijacking, 93
 phishing, 196
Session Initiation Protocol (SIP), 86
SET – eComm protocol, 273
Setting up a Computer Forensics Laboratory, 362–368
Set-top boxes, 98
Seven E's for Security Professionals, 771
Sexting, 104
Sexual exploitation of children, 242
Shellcode, 169
Shocking dimensions of digital signatures, 279
Short Message Service (SMS), 88, 100, 116, 126, 157
 blocker, 105
Shoulder surfing, 63, 134, 218
SIG. *See* Special Interest Group
SIM. *See* Subscriber Identification Module
Similarities between the US regulation and law enforcement of cybercrime in the EU, 249
Simple Mail Transfer Protocol (SMTP), 60, 334
SIP. *See* Session Initiation Protocol
Site cloning, 90
Skiddie, 587
Skimming, 90, 218
Skipping, 63
SLA. *See* Service Level Agreements (SLAs)
Smart chip, 90
SMART forensics tools, 478
Smart hand-held device, 81, 84
Smartphone, 81, 120–121, 431
 forensics, 442–445
Smishing, 101–105
 attacks – safety tips, 104–105
SMS. *See* Short Message Service
SMTP. *See* Simple Mail Transfer Protocol
Smurf attack, 161
Sneakware, 75
Sniffing – network, 51
Social computing, 516
Social engineer, 61–62, 65, 79, 102, 120, 134, 136, 185, 191
 binning, 63
 classification, 62–65
 computer-based, 63–65
 dumpster diving, 63, 65
 E-Mail – attachments, 65
 fake E-Mails, 64
 human-based, 62–63
 impersonation, 62
 pop-up window, 65
 scavenging, 63
 shoulder surfing, 63
 skipping, 63
Social engineers, 61
Social media marketing tools - best practices, 518–522
Social media policy, 518
Social network websites, 192
Social networking sites, 188, 198
 defined, 377
Social Phishing, 193
Social security number (SNN), 187, 236
Software keylogger, 137–139
Software license tracker, 504
Software licensing, 16
Software patent directive, 577
Software patent, 577
Software piracy, 18, 28
Software robots, 71
Software-as-a-service (SaaS) cloud computing, 77
Solving a computer forensics case, 361
Source code, 165
SOX. *See* Sarbanes-Oxley Act
Spam E-Mail, 187, 190
Spam in cyberworld, 31
Spam laws, 238–241
Spam legislation, 36
 in India non-existent, 239
Spam over Internet telephony (SPIT), 104
Spam, 36, 71, 105, 158
SPAMBOT, 188
Spamdexing, 72, 200
Spammers, 18, 131
Spamming, 18–19
SPE. *See* Security Processing Engine
Spear phishing, 195–196
 prevention measures, 196
Special Interest Group (SIG), 188
SPIT. *See* Spam over Internet telephony
Spoofed caller ID, 102
“Spoofed” website, 189, 206
Spoofing, 13, 159
 brand, 187
 E-Mail, 186
SPS. *See* Sanitizing Proxy System
Spy Phishing, 201
Spy phone software, 116
Spyware, 68, 72, 75, 93, 111, 126, 130, 140–142, 145, 152, 198
SQL. *See* Structured Query Language
SSID. *See* Service set identifier
SSL certificate Phishing, 200
SSN. *See* Social Security Number
Stack buffer overflow, 168–169
Stack-smashing attacks, 171
Stash-smashing protector, 171
State Cybersecurity Authority, 293
State Government powers impacted by Indian IT Act amendments, 293–295
State Netizen's Rights Commission, 293
Static free bag, 473
Static IP address – PII, 237
Statistics–cybercrimes in India, 1

- Stealth storage devices, 108–110
 Stealth viruses, 146
 Steganalysis, 158
 tools, 158
 Steganography, 155–157, 369
 and cryptography (difference), 156, 368
 cryptography and digital watermarks, 369
 in forensics context, 454
 tools, 157
 Steps for SQL injection attack, 165–166
 Steps involved in solving a computer forensics case, 361
 Storing and transporting digital evidence, 344–346
 Strong authentication keys, 97
 Strong password, 135
 Structured Query Language (SQL), 164
 block, 168
 commands, 165
 injection, 23, 164–165
 injection attacks – prevention measures, 167
 injection attacks – steps, 165–166
 server penetration – tools, 166–167
 Subscriber Identification Module (SIM), 99–100, 105, 486
 unlocking, 450
 Subversive techniques, 19
 Sudoku, 157
 Summary of changes to the Indian IT Act, 260–263
 Symbian Mobile OS, 86
 Symbian, 98
 SYN attack, 160
 Synthetic Identity Theft, 217
 Synthetically generated images, 458
 System Configuration Phishing, 197
 System integrity tools, 371
 Systematic investigation of cybercrime, 295
- T**
- Tabjacking, 197
 Tablet PC, 83
 Tabnapping, 197
- TCP. *See* Transmission Control Protocol
 TCP SYN flooding, 160
 TCP/IP. *See* Transmission Control Protocol/Internet Protocol
 TDMA. *See* Time Division Multiple Access
 Teardrop attack, 161
 Technical and legal complexities investigating in prosecuting cybercrimes, 306
 Technical aspects in forensics, 551
 Technical challenges faced in digital forensics investigation, 391
 Techniques of identity theft, 218–219
 Techno legal information security, 282
 Techno-crime, 6
 Techno-legal challenges – evidence from hand-held devices, 475–484
 Techno-legal information security, 319
 Telnet protocol, 59–60
 Terrestrial criminal statutes to cyberspace, 307
 Terrestrial laws, 306
 Third Generation (3G), 84
 Threat of cybercrime, 252
 Threatening E-Mails, 254
 Threats – Trojan Horse, 152
 Three Ps of cybercrime – Phishing, Pharming and Phoraging, 198
 Time Division Multiple Access (TDMA), 89, 426, 428–429, 434, 466
 Time stamp – importance in E-Mail investigation, 336
 TLD. *See* Top-level Domain (TLD)
 Toolkit constraints – forensics of hand-held devices, 480–481
 Toolkits for Hand-Held Device Forensics, 463–464
 Tools
 active attacks, 54–58
 with counter-forensics features, 407
 detection of DDoS attacks, 164
 detection of DoS attacks, 164
 DoS attack, 161
- to find Common Vulnerabilities, 127
 hacking wireless networks, 176
 passive attack, 52–53
 password cracking, 133–134
 protect buffer overflow attacks, 171
 for SQL server penetration, 166–167
 steganalysis, 158
 steganography, 157
 used to cover tracks, 128
 vulnerability assessment, 60
 Top 10 cyberthreats, 515
 Top 10 social network sites, 380–381
 Top-level Domain (TLD), 186
 Tracing E-Mails, 336
 Trade secret, 324, 578
 Trademarks, 156, 577–578
 protection, 16
 Traditional forensics vs. remote forensics, 387
 Traditional techniques – wireless network attacks, 176–177
 Traffic analysis, 93
 Traffic data, 287, 294
 Trampoline, 170
 Transborder data flow, 237
 Transmission Control Protocol (TCP), 58, 96, 160
 Transmission Control Protocol/Internet Protocol (TCP/IP), 58, 60, 161
 Transnational nature of cyberspace, 306
 Trends – Mobile and wireless devices, 84–86
 Triad of Information Security, 752
 Triangulation, 90
 Trio of important players – effective fight against cybercrime, 309
 TRIPS – Trade-related Aspects of Intellectual Property Rights, 574
 Trojan Horse, 18, 23, 65, 74–75, 100, 110, 128, 137, 141, 151, 162–163, 191–192, 213, 219
 protection measures, 153–154
 remover software, 154
 Spyware, 202
 threats, 152

- Trojan War, 151
 Trust framework and privacy protection, 231
 Trust seals, 228
 Trusted framework, 231
 Trustworthiness of digital data, 330
Types
 of assurance and compliance, 760–761
 of buffer overflow, 168–170
 of cellular networks, 426–427
 cyberstalkers, 66
 of digital analysis, 350
 DoS attacks, 160–161
 of identity theft, 211–217
 of insiders, 497
 of mobile workers, 172
 password cracking attacks, 134–135
 of Phishing scams, 196–201
Typical E-Mail header – how it looks, 336
- U**
- UBE. *See* Unsolicited bulk E-Mail
 UCE. *See* Unsolicited commercial E-Mail
 UDP. *See* User Datagram Protocol
 UI. *See* User Interface
 Ultramobile PC, 83
 Unauthorized access, 230
 to computer, 229
 Unauthorized use of computing facilities, 246
 Unconventional storage devices, 108–110
 Understanding the Raw Data and its Structure, 390–392
 Uniform resource locator (URL), 50–51
 manipulation Phishing, 193
 Unique Identification Authority of India (UIDAI), 524
 Unique identification card (UID Card), 524
 United Nations Congress – Prevention of Crime and Treatment of Offenders, 229
- Universal Mobile Telecommunications System (UMTS), 426
 Universal serial bus (USB), 434
 drive, 108, 114, 145, 152
 ports, 110
 Unix viruses, 147
 Unlawful access to computer, 229
 Unsolicited bulk E-Mail (UBE), 187, 239
 Unsolicited commercial communications, 239
 Unsolicited commercial E-Mail (UCE), 187
 Unsolicited E-Mails, 67
 Unsolicited messages, 239
 URL. *See* Uniform resource locator
 USB. *See* Universal serial bus (USB)
 Use of data mining in cyberforensics, 318
 Use of personal data, 231
 Usenet Newsgroup as a source of cybercrimes, 30
 User Datagram Protocol (UDP), 58, 96
 User Interface (UI), 126
 User spheres, 515
 Utility patents, 577
- V**
- VAPT. *See* Vulnerability Assessment and Penetration Testing
 Vendor-neutral certifications, 763
 Vendor-specific certifications, 763
 Vicarious liability, 286
 Victimless crimes, 572
 Victims of data security breaches, 303
 Video files, 98
 Video player, 83
 Virginia State Criminal Law, 230
 Virtual keyboard, 69–70
 Virtual private cloud, 76
 Virtual private network (VPN), 85, 93, 114, 174, 751
 Virus attack/dissemination of virus, 18
 Virus (es), 65, 72, 75, 86, 93, 99–101, 111, 137, 151–152, 155, 162, 192, 198
 hoax, 147
- how they spread, 143–144
 types, 146–147
 World's worst attacks, 147
 and worms – difference, 141, 143–145
 Vishing, 101–103, 218
 attacks – safety tips, 103
 Voice Over Internet Protocol (VoIP), 86, 102
 Spam, 104
 Voice-centric security threats, 85
 VoIP. *See* Voice over Internet Protocol
 VPN. *See* Virtual private network (VPN)
 Vulnerabilities
 assessment, 54
 assessment – tools, 60
 networks, 47
 scanners, 562
 scanning and penetration testing, 519
 Vulnerability Assessment and Penetration Testing (VAPT), 761, 769
- W**
- WAN. *See* Wide area network
 WAP. *See* Wireless Application Protocol
 War dialer, 46, 102
 WCDMA. *See* Wideband Code Division Multiple Access
 Weak areas of the ITA 2000, 270
 Weak password, 135
 Web attacks – the motives, 586–587
 Web crawlers, 188
 Web jacking, 18, 22
 Web threats
 to organizations, 505–515
 classified, 506
 Web Trojan Phishing, 197
 Weblink manipulation
 Phishing, 193
 Website forgery Phishing, 193
 Website Spoofing, 191–192
 Well-known ports, 59–60
 WEP. *See* Wired equivalence privacy
 Whaling, 195

White hat hacker, 47, 590
White hat, 48
Why punishing cybercriminals is difficult, 306
Why SPAM is harmful, 240
Wide area network (WAN), 116
Wide Local Area Network (WLAN), 100
Wideband Code Division Multiple Access (WCDMA), 99
Wi-Fi hotspots
 commercial, 174
 free, 174
Wi-Fi protected access (WPA/WPA2), 175
Wi-Fi standard, 173
Wi-Fi, 100, 134, 172–173
WiMax, 174
Windows Active Directory, 93
Windows CE, 98
 mobile OS, 86
Wired equivalence privacy (WEP), 174–175, 179
Wireless Application Protocol (WAP), 93

Wireless cards, 120
Wireless computing, 82
Wireless cracking, 176
Wireless local area network (WLAN), 173–174
Wireless metropolitan area networks, 174
Wireless network attacks, 171–176
 traditional techniques, 176–177
Wireless network, 84
Wireless networks hacking tools, 176
Wireless phone, 82
wireless processing, 89
WLAN. *See* Wide Local Area Network
WLAN. *See* Wireless local area network
Workforce mobility, 560
World Trade Organization (WTO), 574
Worms, 65, 86, 93, 110, 145, 148, 151–152, 162
 and viruses – Difference, 145
World's worst attacks, 148–151

WPA/WPA2 – Wi-Fi protected access, 175

X

X.509 Digital Certificates, 274
X-headers, 336
XSRF – Cross-site request forgery, 192
XSS. *See* Cross-site scripting (XSS)

Y

“You-Can-Spam” Act, 188

Z

Zero-day Attack, 74
Zero-day Emergency Response Team (ZERT), 74
Zero-hour Attack, 74
ZERT. *See* Zero-day Emergency Response Team
Zip drive, 108
Zombie computers, 14
Zombies, 72, 75, 86, 162–163, 201

CYBER SECURITY

Understanding Cyber Crimes, Computer Forensics and Legal Perspectives

About the Book

This book, focusing on **cyberthreats** and **cybersecurity**, provides the much needed awareness in the times of growing cybercrime episodes. The book exhaustively covers important topics on cybersecurity that will help readers to understand the implications of cybercrime. It provides adequate orientation on laws with reference to cybercrime and cybersecurity, taking into account the Indian as well as global scenario. Awareness is created through simple practical tips and tricks. The book will educate the readers on how to avoid becoming victims of cybercrime. Well-presented case illustrations and examples from real life underline the significance of topics addressed in each chapter. The companion CD contains guidelines, checklists and handy reference material as well as laws relevant to the Indian IT Act. This book is authored by an SME from InfoSec domain and co-authored by qualified ethical hacking professional who is also a security certified professional.

Salient Features of the Book

- Authors are industry professionals with extensive experience in the domain of Information Security and Data Privacy.
- A real handy reference that all must have in today's world of cyberthreat.
- Aimed at individuals, students (including those doing law courses), IT professionals and legal professionals for building awareness about cybercrime and cybersecurity.
- Useful for candidates aspiring to appear for international certification exams in the domain of Information Security/IT Security and other related domains.
- All dimensions of cybersecurity discussed – including cyberforensics.
- Complete with an overview of global laws that matter for cybersecurity.
- Understanding of key concepts facilitated through well-illustrated diagrams, tables and vignettes inside the chapters.
- Real-life case illustrations and examples provided to help consolidate understanding of topics presented in each chapter.
- Review questions and reference material pointers at the end of each chapter.



Companion CD contains:

- ✓ Chapters 10–12
- ✓ 23 Useful Appendices

READER LEVEL: Undergraduate/Postgraduate

Visit us at www.wileyindia.com

Wiley India Pvt. Ltd.

4435-36/7, Ansari Road, Daryaganj

New Delhi 110002

Tel: 91-11-43630000

Fax: 91-11-23275895

E-mail: csupport@wiley.com

Website: www.wileyindia.com



WILEY-INDIA

ISBN 978-81-265-2179-1



9 788126 521791