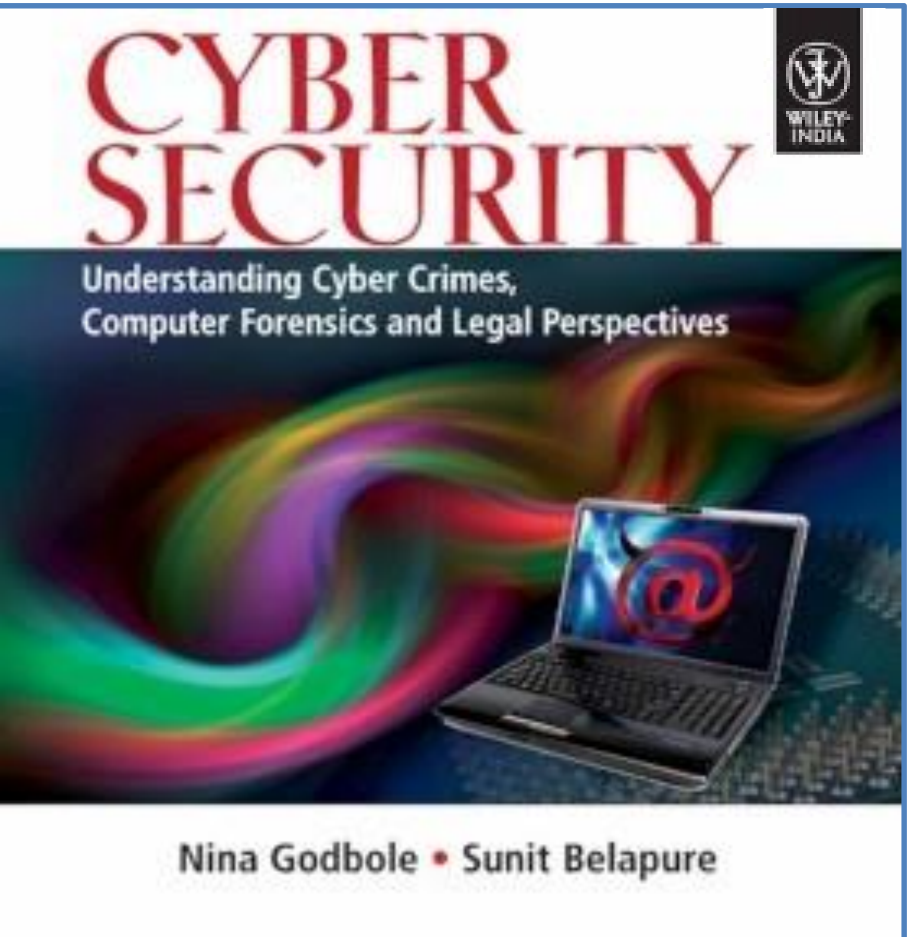
Chapter 1
Introduction to Cybercrime


CYBER SECURITY
Understanding Cyber Crimes, Computer Forensics and Legal Perspectives
WILEY-INDIA
Nina Godbole • Sunit Belapure

Introduction

Internet has undeniably opened a new way of exploitation known as cybercrime involving the use of computers, the Internet, cyberspace and the worldwide web (WWW).

Figure 1, based on a 2008 survey in Australia, shows the cybercrime trend.

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.
- A total of 3,286 Indian websites were hacked in 5 months – between January and June 2009.

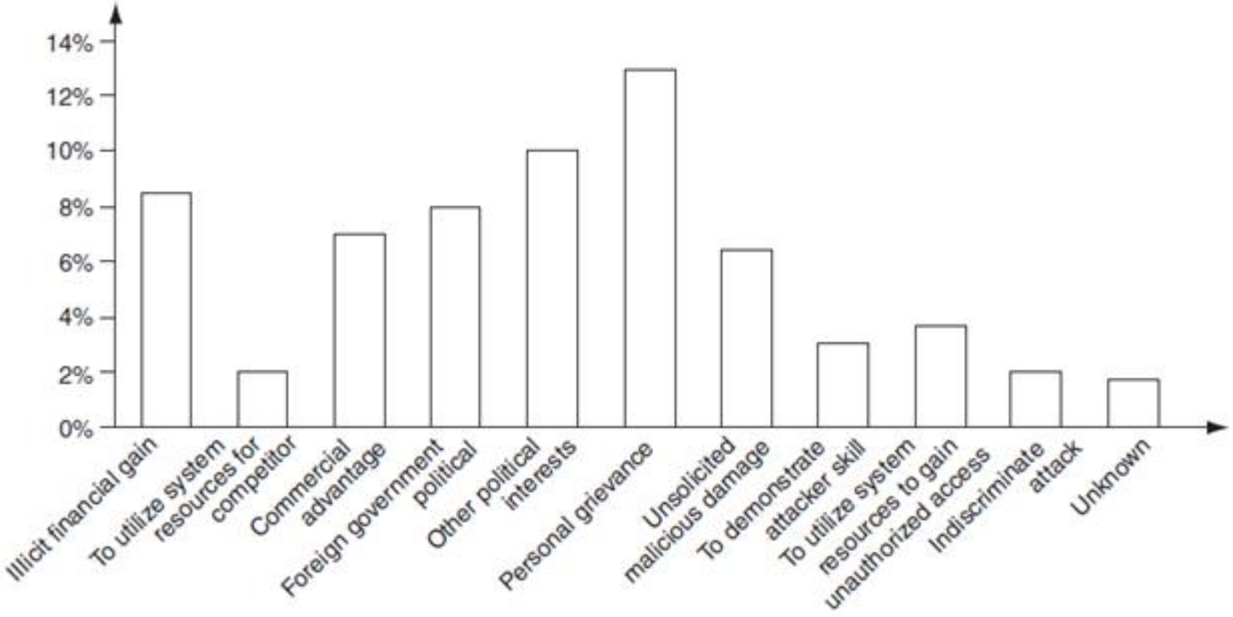


Figure 1 Cybercrime trend.

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).

Cybercrime: Definition and Origins of the Word

The 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.

The term "cybercrime" relates to a number of other terms such as:

- *Computer-related crime*
- *Computer crime*
- *Internet crime*
- *E-crime*
- *High-tech crime*

Two types of attack are prevalent in cybercrimes:

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.
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.

Cybercrimes 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
(d) they are often not clearly illegal.

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*.”

How cybercrimes are planned and how they actually take place

- Cyberterrorists usually use computer as a tool, target or both for their unlawful act to gain information.
- 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), selling illegal articles, pornography/child pornography, etc. This is done using:
  - ➢ Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc.

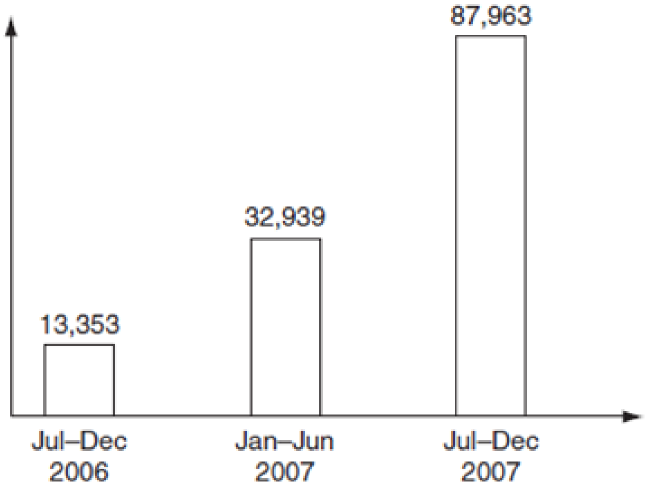


Figure 2 Rise in the number of Phishing hosts.
Source: Symantec (International Telecommunications Society, 17th Biennial Conference, Montreal, Canada, June 24–27, 2008).

Cybercrime and Information Security

Indian Information Technology Act (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.
- Where financial losses to the organization due to insider crimes are concerned, 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.
- For anyone trying to compile data on business impact of cybercrime, there are number of challenges.
  - Organizations do not explicitly incorporate the cost of the vast majority of computer security incidents into their accounting.
  - There is always a difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost.
  - Most organizations abstain from revealing facts and figures about “security incidents” including cybercrime.
  - Organizations perception about “insider attacks” seems to be different than that made out by security solution vendor.
  - Awareness about “data privacy” too tends to be low in most organizations.

Figure 3 shows several categories of incidences – viruses, insider abuse, laptop theft and unauthorized access to systems.

Typical network misuses are for:

- Internet radio
- streaming audio
- streaming video
- file sharing
- instant messaging
- Online gaming
- Online gambling

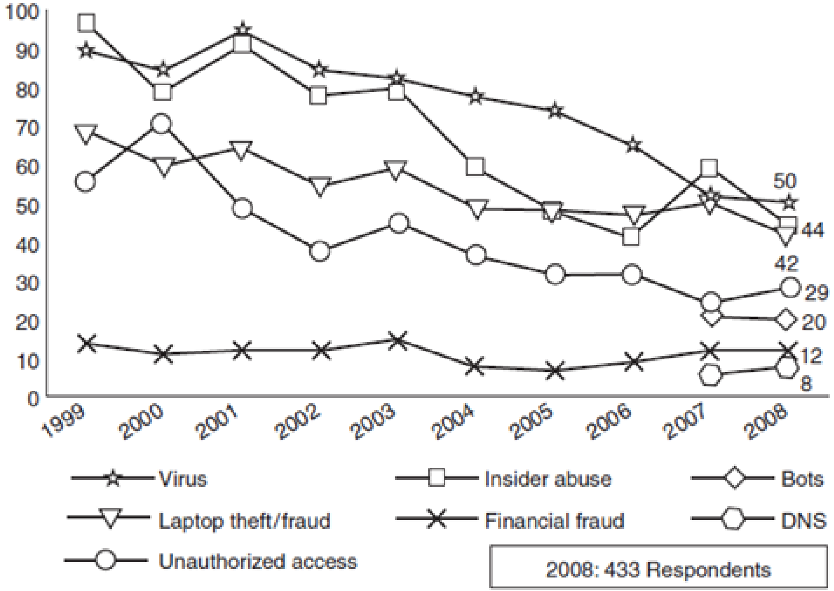


Figure 3 Major types of incidents by percentage.
Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

Who are Cybercriminals?

Cybercriminals are those who conduct activities such 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 to perform criminal acts.

1. Type I: Cybercriminals – hungry for recognition
2. Type II: Cybercriminals – not interested in recognition
3. Type III: Cybercriminals – the insiders

Classifications of Cybercrimes

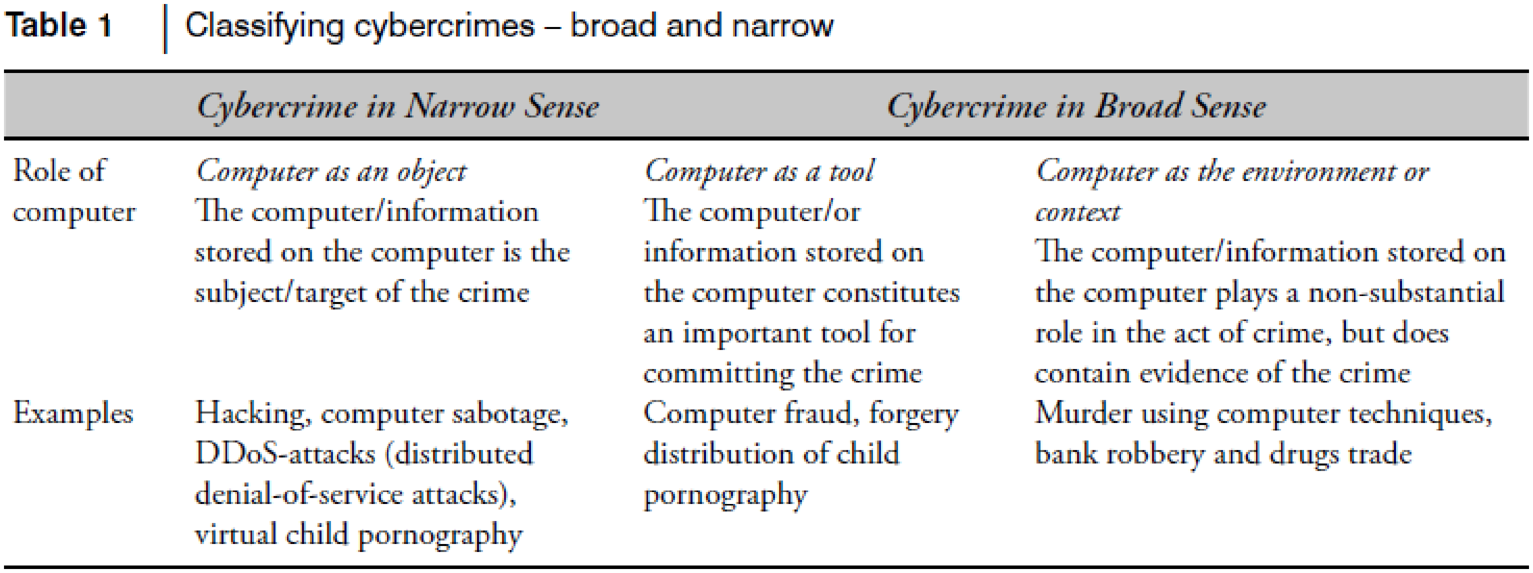


Table 1 | Classifying cybercrimes – broad and narrow

	Cybercrime in Narrow Sense	*Cybercrime in Broad Sense*	
Role of computer	*Computer as an object* The computer/information stored on the computer is the subject/target of the crime	*Computer as a tool* The computer/or information stored on the computer constitutes an important tool for committing the crime	*Computer as the environment or context* 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

Cybercriminals

- Type-I Cybercriminals - hungry for recognition
  - Hobby Hackers
  - IT professionals (Social Engineering is one of the biggest threat)
  - Politically motivated hackers
  - Terrorist organizations
- Type-II Cybercriminals - Not interested in recognition
  - Psychological perverts
  - Financially motivated hackers (Corporate espionage)
  - State sponsored hacking (national espionage, sabotage)
  - Organized criminals
- Type-III Cybercriminals - the insiders
  - Disgruntled or former employees seeking revenge
  - Competing companies using employees to gain economic advantage through damage and/or theft

Classification of Cyber Crimes

Crime is defined as “an act or commission of an act that is forbidden, or omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law”.

Cyber crimes are classified based on the subject of the crime, the person or organization against whom the crime is committed, and the temporal nature of the crimes committed online. Cyber crime is classified into five groups:

Classification of Cyber Crimes

1. Crimes against individuals – These are committed against individuals or their properties. Some examples are:

- Email spoofing and other online fraud
- Phishing, Spear phishing and its various other forms such as Vishing and Smishing
- Spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offences
- Password sniffing

Classification of Cyber Crimes

2. Cybercrime against property

- Credit and fraud
- Intellectual Property crimes
- Internet time theft

Classification of Cyber Crimes

3. Cybercrime against organization

- Unauthorized accessing of computer
- Password sniffing
- Denial of service attacks
- Virus attacks/dissemination of viruses
- E-mail bombing/mail bombs
- Salami attacks/Salami technique
- Logic bomb
- Trojan Horse
- Data diddling
- Crimes emanating from Usenet newsgroup
- Industrial spying/Industrial espionage
- Computer network intrusions
- Software piracy

Classification of Cyber Crimes

4. Crimes against society

- Forgery
- Cyberterrorism
- Web jacking

5. Crimes emanating from Usenet newsgroup

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

Cyber Crimes

E-Mail Spoofing

- A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source.

Spamming

- People who create electronic Spam are called *spammers*.
- Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately.
- Spamming is widely detested, and has been the subject of legislation in many jurisdictions – for example, the CAN-SPAM Act of 2003.

Search engine spamming

- 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.

Cyberdefamation

- "Cyberdefamation" occurs when defamation takes place with the help of computers and/or the 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.

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.

- The law on defamation attempts to create a workable balance between two equally important human rights
    1. *The right to an unimpaired reputation*
    2. *The right to freedom of expression*

Internet Time Theft

- Internet time theft occurs when an unauthorized person uses the Internet hours paid for by another person.
- It comes under hacking because the person gets access to someone else’s ISP user ID and password, either by hacking or by gaining access to it by illegal means

Salami Attack/Salami Technique

- These attacks are used for committing financial crimes.
- No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

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.

Forgery

- Forging counterfeit currency notes, postage and revenue stamps, marksheets, etc. using sophisticated computers, printers and scanners.

Web Jacking

- Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it).

Newsgroup Spam/Crimes Emanating from Usenet Newsgroup

- The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever.
- Spamming of Usenet newsgroups actually predates E-Mail Spam.

Industrial Spying/Industrial Espionage

- “Spies” can get information about product finances, research and development and marketing strategies, an activity known as “industrial spying.”
- “Targeted Attacks” - 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.
- There are two distinct business models for cybercrime applied to industrial spying
  - ➢ Selling Trojan-ware
  - ➢ Selling Stolen Intellectual Property.

Hacking

Hackers, crackers and phrackers 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.

- ➢ 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.

Online Frauds

Types of crimes under the category of hacking

- ✓ Spoofing website and E-Mail security alerts
- ✓ Hoax mails about virus threats
- ✓ lottery frauds
- ✓ Spoofing.

Spoofing websites and E-Mail security threats

- o Fraudsters create authentic looking websites that are actually nothing but a spoof.
- o The purpose of these websites is to make the user enter personal information which is then used to access business and bank accounts
- o This kind of online fraud is common in banking and financial sector.
- o 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.

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.

Lottery frauds

- 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.

Spoofing

- A hacker logs-in to a computer illegally, using a different identity than his own.
- 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.

Pornographic Offenses

"Child pornography" includes:

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.

- ➢ 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.

Software Piracy

- Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

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. 4).

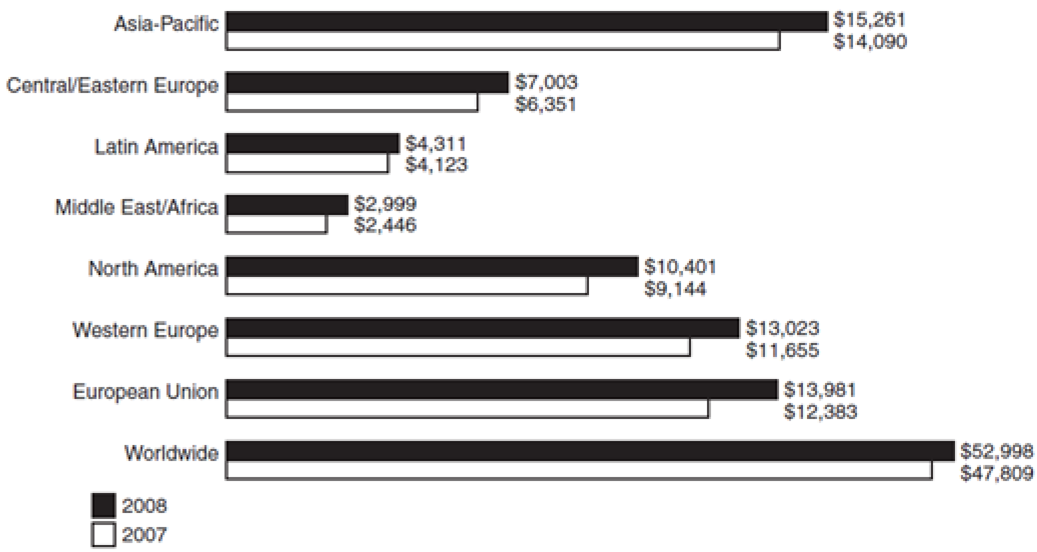


Figure 4 Dollars lost (year 2008) due to (software) piracy – regional scenario. *Source:* BSA-IDC Global 2008 Piracy Study released on May 2009 at the following link: http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf (29 January 2010).

Computer Sabotage

It is the use of the Internet to hinder the normal functioning of a computer system through the introduction of worms, viruses or logic bombs. 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.

E-Mail Bombing/Mail Bombs

- It refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account 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.

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. It is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.

Computer Network Intrusions

- Computer Networks pose a problem by way of security threat because people can get into them from anywhere.
- 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 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.

Credit Card Frauds

- Millions of dollars may be lost annually by consumers who have credit card and calling card numbers stolen from online databases.
- Bulletin boards and other online services are frequent targets for hackers who want to access large databases of credit card information.

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.
- The cyberimpersonator can steal unlimited funds in the victim's name without the victim even knowing about it for months, sometimes even for years!

Cybercrime: The Legal Perspectives

Computer Crime: Criminal Justice Resource Manual (1979)

- The first comprehensive presentation of computer crime
- 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.

Cybercrime:

- outcome of "globalization."
- Globalized information systems accommodate an increasing number of transnational offenses.

This problem can be resolved in two ways:

1. Divide information systems into segments bordered by state boundaries

2. Incorporate the legal system into an integrated entity obliterating these state boundaries

Cybercrimes: An Indian Perspective

India has the fourth highest number of Internet users in the world.

- there are 45 million Internet users in India
  - 37% - from cybercafes
  - 57% of users are between 18 and 35 years.
- A point to note is that the majority of off enders were under 30 years.
  - About 46% cybercrime cases were related to incidents of cyberpornography
  - In over 60% of these cases, off enders were between 18 and 30 years.

Cybercrime and the Indian ITA 2000

- 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.

Hacking and the Indian Law(s)

- Cybercrimes are punishable under two categories: the ITA 2000 and the IPC.
- 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.

A Global Perspective on Cybercrimes

- In Australia, cybercrime has a narrow statutory meaning as used in the *Cyber Crime Act* 2001, which details offenses against computer data and systems.
- 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.
- 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.

  2. In August 18, 2006, there was a news article published “ISPs Wary About ‘Drastic Obligations’ on Web Site Blocking.”

  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.

Cybercrime and the Extended Enterprise

- 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.
- **Extended enterprise** - 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 (Fig. 5).

Cybercrime and extended enterprise

- 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.
- 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 ideas in a collaborative manner.

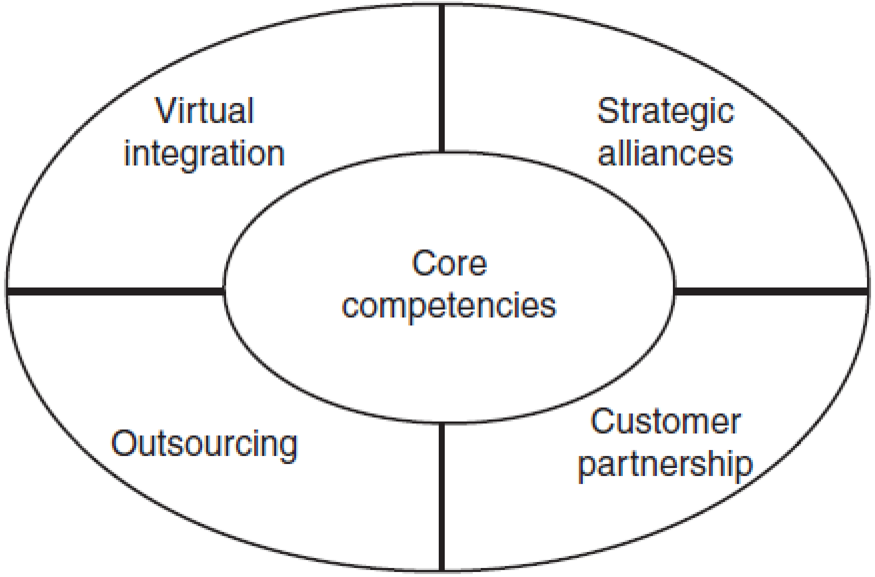


Figure 5 | Extended enterprise.

Cybercrime Era: Survival Mantra for the Netizens

Netizen

- 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!"

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.
7. How do you think cybercrime has relevance in extended enterprise context? Explain.
8. Explain in your own words what you understand about the global cooperation required in fighting against cybercrime.