



COMPUTER SECURITY **FUNDAMENTALS**

THIRD EDITION

CHUCK EASTTOM

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Computer Security Fundamentals

Third Edition

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Computer Security Fundamentals, Third Edition

Copyright © 2016 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5746-3

ISBN-10: 0-7897-5746-X

Library of Congress control number: 2016940227

Printed in the United States of America

First Printing: May 2016

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Executive Editor
Brett Bartow

Acquisitions Editor
Betsy Brown

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Gill Editorial Services

Indexer
Brad Herriman

Proofreader
Paula Lowell

Technical Editor
Dr. Louay Karadsheh

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
Mary Sudul

Contents at a Glance

Introduction	1
1 Introduction to Computer Security	2
2 Networks and the Internet	28
3 Cyber Stalking, Fraud, and Abuse	58
4 Denial of Service Attacks	86
5 Malware	108
6 Techniques Used by Hackers	136
7 Industrial Espionage in Cyberspace	160
8 Encryption	184
9 Computer Security Software	220
10 Security Policies	250
11 Network Scanning and Vulnerability Scanning	276
12 Cyber Terrorism and Information Warfare	310
13 Cyber Detective	338
14 Introduction to Forensics	354
A Glossary	388
B Resources	394
C Answers to the Multiple Choice Questions	396
Index	400

Table of Contents

Introduction	1
Chapter 1: Introduction to Computer Security	2
Introduction	2
How Seriously Should You Take Threats to Network Security?	4
Identifying Types of Threats	6
Malware	6
Compromising System Security	7
DoS Attacks	8
Web Attacks	9
Session Hijacking	11
Insider Threats	11
DNS Poisoning	13
New Attacks	13
Assessing the Likelihood of an Attack on Your Network	14
Basic Security Terminology	15
Hacker Slang	15
Professional Terms	17
Concepts and Approaches	18
How Do Legal Issues Impact Network Security?	19
Online Security Resources	21
CERT	21
Microsoft Security Advisor	21
F-Secure	21
SANS Institute	21
Summary	22
Test Your Skills	22
Chapter 2: Networks and the Internet	28
Introduction	28
Network Basics	29
The Physical Connection: Local Networks	29
Faster Connection Speeds	32

Data Transmission	32
How the Internet Works	34
IP Addresses	34
CIDR	37
Uniform Resource Locators	39
What Is a Packet?	40
Basic Communications	40
History of the Internet	41
Basic Network Utilities	42
IPConfig	43
Ping	45
Tracert	45
Netstat	46
NSLookup	47
Other Network Devices	48
Advanced Network Communications Topics	48
The OSI Model	48
Media Access Control (MAC) Addresses	49
Summary	51
Test Your Skills	51
Chapter 3: Cyber Stalking, Fraud, and Abuse	58
Introduction	58
How Internet Fraud Works	59
Investment Offers	59
Auction Frauds	62
Identity Theft	63
Phishing	65
Cyber Stalking	65
Real Cyber Stalking Cases	66
How to Evaluate Cyber Stalking	69
Crimes Against Children	70
Laws About Internet Fraud	72
Protecting Yourself Against Cyber Crime	72
Protecting Against Investment Fraud	72

Protecting Against Identity Theft	73
Secure Browser Settings	74
Summary	79
Test Your Skills	79
Chapter 4: Denial of Service Attacks	86
Introduction	86
DoS	87
Illustrating an Attack	87
Common Tools Used for DoS	89
DoS Weaknesses	91
Specific DoS Attacks	91
Land Attack	97
DDoS	97
Summary	101
Test Your Skills	101
Chapter 5: Malware	108
Introduction	108
Viruses	109
How a Virus Spreads	109
Types of Viruses	110
Virus Examples	111
Rombertik	111
Gameover Zeus	111
CryptoLocker and CryptoWall	111
FakeAV	112
MacDefender	112
Troj/Invo-Zip	112
W32/Netsky-P	112
The Sobig Virus	113
The Mimail Virus	114
The Bagle Virus	114
A Nonvirus Virus	114
Flame	115

Rules for Avoiding Viruses	115
Trojan Horses.	116
The Buffer-Overflow Attack	119
The Sasser Virus/Buffer Overflow	120
Spyware	121
Legal Uses of Spyware	121
How Is Spyware Delivered to a Target System?	122
Obtaining Spyware Software	122
Other Forms of Malware	124
Rootkit	124
Malicious Web-Based Code.	125
Logic Bombs	125
Spam	126
Advanced Persistent Threats	126
Detecting and Eliminating Viruses and Spyware	127
Antivirus Software	127
Antispyware Software	128
Remediation Steps	128
Summary	130
Test Your Skills	130
Chapter 6: Techniques Used by Hackers	136
Introduction	136
Basic Terminology.	137
The Reconnaissance Phase	137
Passive Scanning Techniques	137
Active Scanning Techniques	139
Actual Attacks	144
SQL Script Injection	144
Cross-Site Scripting	146
Password Cracking	146
Malware Creation	148
Windows Hacking Techniques	149

Penetration Testing	151
NIST 800-115.	151
National Security Agency Information Assessment Methodology	151
PCI Penetration Testing Standard	152
Summary	154
Test Your Skills	154
Chapter 7: Industrial Espionage in Cyberspace	160
Introduction	160
What Is Industrial Espionage?	161
Information as an Asset	162
Real-World Examples of Industrial Espionage	165
Example 1: Houston Astros	165
Example 2: University Trade Secrets.	165
Example 3: VIA Technology	166
Example 4: General Motors	166
Example 5: Bloomberg, Inc.	167
Example 6: Interactive Television Technologies, Inc.	167
Trends in Industrial Espionage.	167
Industrial Espionage and You	168
How Does Espionage Occur?	168
Low-Tech Industrial Espionage	168
Spyware Used in Industrial Espionage	171
Steganography Used in Industrial Espionage	171
Phone Taps and Bugs.	172
Protecting Against Industrial Espionage	172
Industrial Espionage Act.	175
Spear Phishing.	175
Summary	177
Test Your Skills	177

Chapter 8: Encryption	184
Introduction	184
Cryptography Basics	185
History of Encryption	185
The Caesar Cipher	188
Atbash	189
Multi-Alphabet Substitution	189
Rail Fence	190
Enigma	191
Binary Operations	192
Modern Methods	193
Single-Key (Symmetric) Encryption	194
Modification of Symmetric Methods	200
Public Key (Asymmetric) Encryption	201
PGP	205
Legitimate Versus Fraudulent Encryption Methods	206
Digital Signatures	207
Hashing	207
MD5	208
SHA	208
RipeMD	208
MAC and HMAC	208
Rainbow Tables	209
Steganography	210
Historical Steganography	211
Methods and Tools	211
Cryptanalysis	211
Frequency Analysis	212
Modern Methods	212
Cryptography Used on the Internet	213
Summary	214
Test Your Skills	214

Chapter 9: Computer Security Technology	220
Introduction	220
Virus Scanners	221
How Does a Virus Scanner Work?	221
Virus-Scanning Techniques	222
Commercial Antivirus Software	224
Firewalls	224
Benefits and Limitation of Firewalls	224
Firewall Types and Components	225
Firewall Configurations	226
Commercial and Free Firewall Products	227
Firewall Logs	228
Antispyware	228
IDS	229
IDS Categorization	229
Identifying an Intrusion	230
IDS Elements	230
Snort	231
Honey Pots	235
Database Activity Monitoring	235
Other Preemptive Techniques	235
Authentication	236
Digital Certificates	238
SSL/TLS	240
Virtual Private Networks	242
Point-to-Point Tunneling Protocol	242
Layer 2 Tunneling Protocol	243
IPsec	243
Wi-Fi Security	244
Wired Equivalent Privacy	244
Wi-Fi Protected Access	244
WPA2	244
Summary	245
Test Your Skills	245

Chapter 10: Security Policies	250
Introduction	250
What Is a Policy?	251
Defining User Policies	251
Passwords	252
Internet Use	253
Email Usage	254
Installing/Uninstalling Software	255
Instant Messaging	255
Desktop Configuration	256
Bring Your Own Device	256
Final Thoughts on User Policies	257
Defining System Administration Policies	258
New Employees	258
Departing Employees	258
Change Requests	259
Security Breaches	261
Virus Infection	261
DoS Attacks	262
Intrusion by a Hacker	262
Defining Access Control	263
Developmental Policies	264
Standards, Guidelines, and Procedures	264
Data Classification	265
DoD Clearances	265
Disaster Recovery	266
Disaster Recovery Plan	266
Business Continuity Plan	266
Impact Analysis?	266
Fault Tolerance	267
Important Laws	268
HIPAA	269
Sarbanes-Oxley	269
Payment Card Industry Data Security Standards	269

Summary	270
Test Your Skills	270
Chapter 11: Network Scanning and Vulnerability Scanning	276
Introduction	276
Basics of Assessing a System	277
Patch	277
Ports	278
Protect	281
Policies	282
Probe	284
Physical	284
Securing Computer Systems	285
Securing an Individual Workstation	285
Securing a Server	287
Securing a Network	289
Scanning Your Network	291
MBSA	291
NESSUS	293
Getting Professional Help	298
Summary	302
Test Your Skills	302
Chapter 12: Cyber Terrorism and Information Warfare	310
Introduction	310
Actual Cases of Cyber Terrorism	311
The Chinese Eagle Union	312
China's Advanced Persistent Threat	312
India and Pakistan	313
Russian Hackers	313
Weapons of Cyber Warfare	313
Stuxnet	313
Flame	314
StopGeorgia.ru Malware	314
FinFisher	314

BlackEnergy	315
NSA ANT Catalog	315
Economic Attacks	315
Military Operations Attacks	317
General Attacks	318
Supervisory Control and Data Acquisitions (SCADA).	318
Information Warfare.	319
Propaganda	319
Information Control	320
Disinformation	322
Actual Cases	322
Future Trends.	326
Positive Trends	326
Negative Trends	328
Defense Against Cyber Terrorism	329
Terrorist Recruiting and Communication.	330
TOR and the Dark Web.	330
Summary	333
Test Your Skills	333
Chapter 13: Cyber Detective	338
Introduction	338
General Searches	339
Court Records and Criminal Checks	342
Sex Offender Registries	342
Civil Court Records	344
Other Resources	345
Usenet	346
Summary	348
Test Your Skills	348

Chapter 14: Introduction to Forensics	354
Introduction	354
General Guidelines	355
Don't Touch the Suspect Drive	355
Image a Drive with Forensic Toolkit.	356
Can You Ever Conduct Forensics on a Live Machine?	358
Document Trail	359
Secure the Evidence	359
Chain of Custody.	360
FBI Forensics Guidelines	360
U.S. Secret Service Forensics Guidelines.	361
EU Evidence Gathering.	362
Scientific Working Group on Digital Evidence	362
Locard's Principle of Transference	363
Tools.	363
Finding Evidence on the PC.	364
Finding Evidence in the Browser	364
Finding Evidence in System Logs	365
Windows Logs	365
Linux Logs	366
Getting Back Deleted Files	366
Operating System Utilities	369
Net Sessions	369
Openfiles	369
Fc	370
Netstat	370
The Windows Registry	371
Specific Entries	372
Mobile Forensics: Cell Phone Concepts	375
Cell Concepts Module	375
Cellular Networks	376
iOS	377
Android.	377
Windows	378
What You Should Look For	379

The Need for Forensic Certification	380
Expert Witnesses.	381
Federal Rule 702	381
Daubert.	382
Additional Types of Forensics	382
Network Forensics	382
Virtual Forensics	382
Summary	385
Test Your Skills	385
Appendix A: Glossary	388
Appendix B: Resources	394
General Computer Crime and Cyber Terrorism	394
General Knowledge.	394
Cyber Stalking	394
Identity Theft	394
Port Scanners and Sniffers.	395
Password Crackers.	395
Countermeasures	395
Cyber Investigation Tools	395
General Tools.	395
Virus Research.	395
Appendix C: Answers to the Multiple Choice Questions	396
Index	400

About the Author

Chuck Easttom is a computer security and forensics expert. He has authored 20 books, including several on computer security, forensics, and cryptography. He holds 6 patents and 40 computer certifications, including many security and forensics certifications. He has conducted training for law enforcement, federal agencies, and friendly foreign governments. He frequently works as an expert witness in computer-related cases. He is also a frequent speaker on computer security topics at a variety of security-related conferences. You can visit his website at www.chuckeasttom.com.

About the Technical Reviewer

Dr. Louay Karadsheh has a Doctorate of Management in information technology from Lawrence Technological University, Southfield, Michigan. His research interest includes cloud computing, information assurance, knowledge management, and risk management. Dr. Karadsheh has published 11 articles in refereed journals and international conference proceedings and has extensive knowledge in operating system, networking, and security. Dr. Karadsheh has provided technical edits/reviews for several major publishing companies, including Pearson and Cengage Learning. He holds CISSP, CEH, CASP, CCSK, CCE, Security+, VCA-C, VCA-DCV, SCNP, Network+, and Mobility+ certifications.

Dedication

*This book is dedicated to my wife, Teresa,
who has helped me become who I am.*

Acknowledgments

The creation of a book is not a simple process and requires the talents and dedication from many people to make it happen. With this in mind, I would like to thank the folks at Pearson for their commitment to this project.

Specifically, I would like to say thanks to Betsy Brown for overseeing the project and keeping things moving.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *Computer Security Fundamentals* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789757463 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

It has been more than 10 years since the publication of the original edition of this book. A great deal has happened in the world of computer security since that time. This edition is updated to include newer information, updated issues, and revised content.

The real question is: Who is this book for? This book is a guide for any computer-savvy person. That means system administrators who are not security experts or anyone who has a working knowledge of computers and wishes to know more about cyber crime and terrorism could find this book useful. However, the core audience will be students who wish to take a first course in security but may not have a thorough background in computer networks. The book is in textbook format, making it ideal for introductory computer security courses that have no specific prerequisites. That lack of prerequisites means that people outside the normal computer science and computer information systems departments could also avail themselves of a course based on this book. This might be of particular interest to law enforcement officers, criminal justice majors, and even business majors with an interest in computer security.

As was previously mentioned, this book is intended as an introductory computer security book. In addition to the numerous end notes, the appendixes will guide you to a plethora of additional resources. There are also review questions and practice exercises with every chapter. Appendix C contains the answers to the multiple choice questions for your review. Exercises and projects don't have a single answer. They are intended to encourage the reader to explore, so answers will vary.

This book is not a cookbook for hackers. You will see exactly how hackers target a system and get information about it. You will also see step-by-step instructions on how to use some password-cracking utilities and some network-scanning utilities. You will also be given a reasonably in-depth explanation of various hacking attacks. However, you won't see a specific step-by-step recipe for executing an attack.

This book assumes that you are a competent computer user. That means you have used a computer at work and at home, are comfortable with email and web browsers, and know what words like RAM and USB mean. For instructors considering this as a textbook, that means students will have had some basic understanding of PCs but need not have had formal computer courses. For this reason, there is a chapter on basic networking concepts to get you up to speed. For readers with more knowledge, such as system administrators, you will find some chapters of more use to you than others. Feel free to simply skim any chapter that you feel is too elementary for you.

Chapter 7

Industrial Espionage in Cyberspace

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Know what is meant by industrial espionage
- Understand the low-technology methods used to attempt industrial espionage
- Be aware of how spyware is used in espionage
- Know how to protect a system from espionage

Introduction

When you hear the word *espionage*, perhaps you conjure up a number of exciting and glamorous images. Perhaps you have visions of a well-dressed man who drinks martinis, shaken but not stirred, traveling to glamorous locations with equally glamorous travel companions. Or perhaps you envision some exciting covert operation with high-speed car chases and guns blazing in faraway exotic lands. Contrary to popular media portrayals, espionage is often much less exciting than those visions. The ultimate goal of espionage is to obtain information that would not otherwise be made available. Generally, espionage is best done with as little fanfare as possible. Blazing gun battles and glamorous locations tend to be the antithesis of intelligence gathering. Rather, information is the goal. If possible, it is best to obtain that information without the target organization even realizing that its information has been compromised.

Many people assume that such spying is only engaged in by governments, intelligence agencies, and nefarious international organizations, such as Al Qaida or ISIS. While those entities do indeed engage in espionage, they are certainly not the only organizations that do so. The aforementioned organizations desire to acquire information for political and military goals. However, economic goals are also dependent on accurate and often sensitive data. With billions of dollars at stake, private companies can become engaged in industrial espionage as either a target or a perpetrator. What company would not like to know exactly what its competitor is doing? In fact, corporate or economic espionage is on the rise.

Corporate or economic espionage is a growing problem, but it can be difficult to accurately assess just how great a problem it is. Companies that perpetrate corporate espionage do not share the fact that they do it, for obvious reasons. Companies that are victims of such espionage often do not wish to reveal that fact either. Revealing that their security was compromised could have a negative impact on their stock value. It is also possible, in certain cases, that such a breach of security might open the company to liability claims from customers whose data may have been compromised. For these reasons, companies often are hesitant to disclose any industrial espionage activities. Because you will want to protect yourself and your company, it is important that you learn about espionage methods and protections. In the exercises at the end of this chapter, you will run antispyware, key loggers, and screen-capture software so that you are aware of how they work and, hence, will be cognizant of the risks they pose. While we did cover those in previous chapters, we will expand on that in this chapter's exercises.

What Is Industrial Espionage?

Industrial espionage is simply the use of spying techniques to find out key information that is of economic value. Such data might include details on a competitor's new project, a list of a competitor's clients, research data, or any information that might give the spying organization an economic advantage. While the rationale for corporate espionage is different from military espionage, corporate techniques are often the same as those methods employed by intelligence agencies and can include electronic monitoring, photocopying files, or compromising a member of the target organization. Not only does economic espionage use the same techniques as intelligence agencies, but it often also uses the same people. There have been a number of incidents in which former intelligence agents were found working in corporate espionage. When such individuals bring their skills and training to the world of corporate espionage, the situation becomes much more difficult for computer security experts.

In Practice**Leaving with Sensitive Data**

While various computer experts and government agencies attempt to estimate the impact and spread of corporate espionage, its very nature makes accurate estimates impossible. Not only do the perpetrators not wish to disclose their crimes, but often the victims will not disclose the event either. However, anecdotal evidence would suggest that the most common form of espionage is simply an employee who quits, takes a job with another firm, and leaves with sensitive data. In many cases, these employees choose data that is readily available within the company and, as such, the data is considered a “gray area” as to its confidentiality. For example, a salesperson may leave with a printout of contacts and customers so that he can solicit them on behalf of the next employer. It is critical that you have a very well-worded nondisclosure and noncompete agreement with all employees. It is best to solicit the services of an employment attorney to draw up this agreement. Additionally, you might consider limiting an employee’s access to data prior to terminating his employment. You should also conduct exit interviews and consider confiscating items such as company phone books, which may at first seem insignificant but which could contain data useful to another company. It is also the case that thumb drives, smart phones, and other technologies provide a method for taking data out of a company. Some companies restrict the use of these devices.

Information as an Asset

Many people are used to viewing tangible objects as assets but have difficulty appreciating how mere information can be a real asset. Companies spend billions of dollars every year on research and development. The discovered information is worth at least the amount of resources taken to derive the information plus the economic gain produced by the information. For example, if a company spends \$200,000 researching a process that will in turn generate \$1 million in revenue, then that data is worth at least \$1.2 million. You can think of this economic gain as a simple equation:

$$VI \text{ (value of information)} = C \text{ (cost to produce)} + VG \text{ (value gained)}$$

While some people are not yet fully cognizant of the concept, data does indeed represent a valuable asset. When we speak of the “information age” or our “information-based economy,” it is important to realize that these terms are not just buzzwords. Information is a real commodity. It is as much an economic asset as any other item in the company’s possession. In fact, it is most often the case that the data residing on a company’s computer is worth far more than the hardware and software of the computer system itself. It is certainly the case that the data is much more difficult to replace than the computer hardware and software.

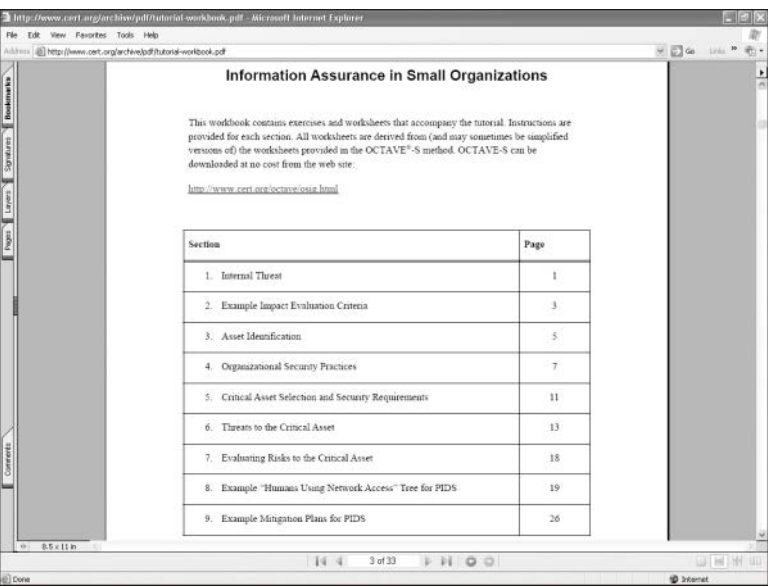
To help you truly appreciate the concept of information as a commodity, consider the process of earning a college degree. You spend four years sitting in various classrooms. You pay a significant amount of money for the privilege of sitting in a room and listening to someone speak at length on

some topic. At the end of the four years, the only tangible product you receive is a single piece of paper. Surely you can get a piece of paper for far less cost and with much less effort. What you actually paid for was the information you received. The same is true of the value of many professions. Doctors, attorneys, engineers, consultants, managers, and so forth all are consulted for their expert information. Information itself is the valuable commodity.

The data stored in computer systems has a high value for two reasons. First, there is a great deal of time and effort that goes into creating and analyzing the data. If you spend six months with a team of five people gathering and analyzing information, then that information is worth at least an amount equal to the salaries and benefits of those people for that length of time. Second, data often has intrinsic value, apart from the time and effort spent acquiring those facts. If the facts are about a proprietary process, invention, or algorithm, its value is obvious. However, any data that might provide a competitive edge is inherently valuable. For example, insurance companies frequently employ teams of statisticians and actuaries who use the latest technology to try to predict the risks associated with any given group of potential insureds. The resulting statistical information might be quite valuable to a competing insurance company. Even a customer contact list has a certain inherent value.

Thus, as you work in the computer security field, always keep in mind that any data that might have economic value is an asset to your organization and that such data provides an attractive target for any competitors who may not have ethical inhibitions against using espionage. If your company management thinks that this threat is not real, then they are very much mistaken. Any company is a potential victim of corporate espionage. You should take steps to protect your valuable information—and the first critical step in this process is asset identification.

Asset identification is the process of listing the assets that you believe support your organization. This list should include things that impact direct day-to-day operations as well as those that are tied to your company's services or products. The CERT website (http://people.tuke.sk/dezider.guspan/security/___bezpecnost%20OCTAVE%20CERT/Tutorial%20Workbook%20-tutorial-workbook.pdf) offers a very useful worksheet that you can use to itemize the assets in your organization. This workbook also offers a number of other useful worksheets for assuring information security within your organization. As the table of contents in Figure 7.1 shows, this workbook is also a tutorial that steps you through all the information security considerations.



The screenshot shows a Microsoft Internet Explorer window with the address bar displaying <http://www.cert.org/archive/pdf/tutorial-workbook.pdf>. The page title is "Information Assurance in Small Organizations". The main content area contains a paragraph explaining that the workbook contains exercises and worksheets that accompany the tutorial, and that all worksheets are derived from (and may sometimes be simplified versions of) the worksheets provided in the OCTAVE-S method. A link to <http://www.cert.org/octave/octave.html> is provided. Below the text is a table of contents with two columns: "Section" and "Page". The table lists nine sections, starting with "1. Internal Threat" on page 1 and ending with "9. Example Mitigation Plans for PIDS" on page 26. The browser's status bar at the bottom shows "Done" and "Internet".

Section	Page
1. Internal Threat	1
2. Example Impact Evaluation Criteria	3
3. Asset Identification	5
4. Organizational Security Practices	7
5. Critical Asset Selection and Security Requirements	11
6. Threats to the Critical Asset	13
7. Evaluating Risks to the Critical Asset	18
8. Example "Humans Using Network Access" Tree for PIDS	19
9. Example Mitigation Plans for PIDS	26

FIGURE 7.1 Table of contents from the CERT Information Assurance in Small Organizations workbook.

Table 7.1 is a variation on the worksheet provided by CERT. Armed with this table and based on your knowledge and experience with the company, you can complete your asset identification following the steps outlined below.

TABLE 7.1 Asset Identification Worksheet

Information	Systems	Services and Applications	Other Assets	

1. In the first column of the table, list the information assets. You should list the types of information used by people in your company—the information people need to do their jobs. Examples are product designs, software programs, system designs, documentation, customer orders, and personnel data.

2. For each entry in the Information column, fill in the names of the systems on which the information resides. In each case, ask yourself which systems people need to perform their jobs.
3. For each entry in the Information column, fill in the names of the related applications and services. In each case, ask yourself what applications or services are needed for individuals to perform their jobs.
4. In the last column, list any other assets that may or may not be directly related to the other three columns. Examples are databases with customer information, systems used in production, word processors used to produce documentation, compilers used by programmers, and human resources systems.

Once you complete the proceeding steps and fill out the Asset Identification worksheet, you will have a good understanding of the critical assets for your organization. With this information, you will know how best to devote your defensive efforts. Some specific protective steps will be examined later in this chapter.

Real-World Examples of Industrial Espionage

Now that you have been introduced to the concept of corporate espionage, let's look at five actual cases. These case studies are of real-world espionage found in various news sources. This section should give you an idea of what types of espionage activities actually occur. Note that while some of these cases are a bit old, they do illustrate the way industrial espionage is done. And it is frequently the case that details of an industrial espionage incident do not emerge until many years later, if at all.

Example 1: Houston Astros

In 2015 the Houston Astros baseball team's scouting and team information database was stolen. It is alleged that it was stolen by members of the St. Louis Cardinals. The Houston Astros have a proprietary internal computer system they named Ground Control. It has notes on players and potential trading of players.

The Astros general manager, Jeff Luhnow, had previously worked for the Cardinals, and when he came to work for the Astros, he also brought along some of his staff. Initial reports are that either Mr. Luhnow or one of his staff used a password similar to what he had used with the Cardinals. This allowed someone associated with the Cardinals to guess the password and access the Houston Astros database.

Example 2: University Trade Secrets

In May 2015, Professor Hao Zhang of Tianjin University and five other individuals were arrested and charged with stealing trade secrets for use by universities controlled by the Chinese government. The secrets stolen included research and development on thin-film bulk acoustic resonator (FBAR) technology.

The details of FBAR technology are not important for our discussion of this case of industrial espionage, but I will provide you with a brief description: It is essentially a device that has material located between two electrodes and acoustically isolated from the medium it is in. This is commonly used as a radio frequency filter in cell phones.

Example 3: VIA Technology

VIA Technology actually provides two examples of industrial espionage. In the first instance, the chief executive officer (CEO) of the firm, which was based in Taipei, was indicted for copyright infringement for allegedly stealing technology from one of his own customers, a networking company called D-Link (Network World Fusion, 2003).

According to the allegations, VIA engineer Jeremy Chang left VIA to work for D-Link. For several months while at D-Link, Chang continued to receive a paycheck from VIA. Then he promptly resigned from D-Link and returned to VIA. Once Chang rejoined VIA, a D-Link document that detailed one of its simulation programs for testing integrated circuits was posted to an FTP server owned by VIA.

The prosecutors allege that Chang continued to receive a check from VIA because he had never really resigned. They allege that Chang was in fact a “plant” sent to D-Link to acquire D-Link’s technology for VIA. VIA maintains that his continuation to receive a check was simply an oversight, and Chang denies that he posted the document in question. Whatever the truth of the case, it should make any employer think twice about hiring decisions and nondisclosure agreements.

To make matters worse for VIA, another company accused VIA of stealing code for its optical readers. In both cases, the story of the possible theft of technology alone has had a negative impact on the stock value of both companies.

Example 4: General Motors

In 1993, General Motors (GM) and one of its partners began to investigate a former executive, Inaki Lopez. GM alleged that Lopez and seven other former GM employees had transferred GM proprietary information to Volkswagen (VW) in Germany via GM’s own network (Brinks et al., 2003). The information allegedly stolen included component price data, proprietary construction plans, internal cost calculations, and a purchasing list.

In 1996, GM followed up the ongoing criminal investigation with civil litigation against Lopez, VW, and the other employees. In November 1996, GM expanded its legal battle by invoking the various Racketeer Influenced and Corrupt Organizations Act (RICO) statutes, originally intended to be used against organized crime conspiracies (*Economist*, 1996). By May 2000, a federal grand jury indicted Lopez on six counts related to fraud and racketeering. As of this writing, the case is not resolved (*USA Today*, 2000). At the time Lopez was indicted, he was residing in Spain, and the U.S. Justice Department was negotiating for his extradition. Thus, you can see that corporate espionage is neither new nor restricted to technology companies.

Example 5: Bloomberg, Inc.

According to the *American Bar Association Journal* (2003), in August 2003, Oleg Zezev, a 29-year-old PC technician from Kazakhstan, broke into the Bloomberg Inc. computer system and used the alias Alex to obtain information and then blackmail the firm.

Zezev entered Bloomberg's computer system and accessed various accounts, including Michael Bloomberg's (CEO and founder of Bloomberg L.P.) personal account as well as accounts for other Bloomberg employees and customers. Zezev copied information from these accounts, including email inbox screens, Michael Bloomberg's credit card numbers, and screens relating to the internal functions of Bloomberg. He also copied internal information that was only accessible by Bloomberg employees.

Zezev then threatened to expose the data he had stolen to the public and, in essence, tell everyone exactly how he had broken into Bloomberg's network unless he received \$200,000.

After deliberating for less than six hours, the jury in the U.S. District Court in Manhattan found the perpetrator guilty of all four charges: conspiracy, attempted extortion, sending threatening electronic messages, and computer intrusion. Although this is not industrial espionage in the classic sense, it does illustrate the compromising situations in which a company and its employees can be placed when security is breached.

Example 6: Interactive Television Technologies, Inc.

On August 13, 1998, someone broke into the computer systems of Interactive Television Technologies, Inc. and stole the data for a project the company was working on (Secure Telecom, 1998). That project involved four years of intense research and a substantial financial investment. The product was to be a way whereby anyone with a television could have Internet access via the Web. This product, code named "Butler," would have been worth a substantial amount to its inventors. However, with all the research material stolen, it was only a matter of time before several other companies came out with competing products, thus preventing Interactive Television Technologies from pursuing a patent.

To date, no arrests have been made and no leads are available in this case. This situation was a case of very skillful hackers breaking into a computer system and taking exactly what they needed. One can only speculate about their motives. They may well have sold the research data to competitors of Interactive Television Technologies, or they may have simply put the data out in the open via the Internet. Whatever the motives or profits for the perpetrators, the outcome for the victim company was catastrophic.

Trends in Industrial Espionage

While the cases just discussed range over a number of years, the problem is not abating. In fact, according to a CNN report, 2015 saw a 53% increase in cases of industrial espionage. The FBI conducted a survey of 165 companies and found that half of those companies had been the victim of industrial espionage of some type. A significant number of industrial espionage cases involve insider threats.

Industrial Espionage and You

These cases notwithstanding, most companies will deny involvement in anything that even hints at espionage. However, not all companies are quite so shy about the issue. Larry Ellison, CEO of Oracle Corporation, has openly defended his decision to hire private investigators to sift through Microsoft garbage in an attempt to garner information (CNET News, 2001). Clearly, espionage is no longer a problem just for governments and defense contractors. It is a very real concern in the modern business world. The savvy computer security professional will be aware of this concern and will take the appropriate proactive steps.

How Does Espionage Occur?

There are two ways that espionage can occur. An easy, low-technology avenue would be for current or former employees to simply take the data or for someone to use social engineering methods (discussed in Chapter 3, “Cyber Stalking, Fraud, and Abuse”) to extract data from unsuspecting company employees. The second, more technology-oriented method is for the individuals to use spyware, which includes the use of cookies and key loggers. There are other technological methods we will discuss.

Low-Tech Industrial Espionage

Corporate espionage can occur without the benefit of computers or the Internet. Disgruntled former (or current) employees can copy sensitive documents, divulge corporate strategies and plans, or perhaps reveal sensitive information. In fact, whether the method used is technological or not, disgruntled employees are the single greatest security risk to any organization. A corporate spy need not hack into a system in order to obtain sensitive and confidential information if an employee is willing to simply hand over the information. Just as with military and political espionage, the motives for the employee to divulge the information vary. Some engage in such acts for obvious financial gains. Others may elect to reveal company secrets merely because they are angry over some injustice (real or imagined). Whatever the motive, any organization has to be cognizant of the fact that it has any number of employees who may be unhappy with some situation and have the potential to divulge confidential information.

Certainly, one can obtain information without the benefit of modern technology; however, computer technology (and various computer-related tactics) can certainly assist in corporate espionage, even if only in a peripheral manner. Some incidents of industrial espionage are conducted with technology that requires little skill on the part of the perpetrator, as illustrated in Figures 7.2 and 7.3. This technology can include using universal serial bus (USB) flash drives, compact discs (CDs), or other portable media to take information out of the organization. Even disgruntled employees who wish to undermine the company or make a profit for themselves will find it easier to burn a wealth of data onto a CD and carry that out in their coat pocket rather than attempt to photocopy thousands of documents and smuggle them out. And the new USB flash drives, smaller than your average key chain, are a dream come true for corporate spies. These drives can plug into any USB port and store a tremendous amount of data. As of this writing, one can easily purchase small portable devices capable of holding 2 terabytes or more of data.



FIGURE 7.2 Low-tech espionage is easy.



FIGURE 7.3 Low-tech espionage is portable.

While information can be taken from your company without overt hacking of the system, you should keep in mind that if your system is unsecure, it is entirely possible that an outside party would compromise your system and obtain that information without an employee as an accomplice. In addition to these methods, there are other low-tech, or virtually “no-tech,” methods used to extract information. *Social engineering*, which was discussed at length in Chapter 3, is the process of talking a person into giving up information she otherwise would not divulge. This technique can be applied to industrial espionage in a number of ways.

The first and most obvious use of social engineering in industrial espionage is in direct conversation in which the perpetrator attempts to get the targeted employee to reveal sensitive data. As illustrated in Figure 7.4, employees will often inadvertently divulge information to a supplier, vendor, or salesperson without thinking the information is important or that it could be given to anyone. This involves simply trying to get the target to talk more than they should. In 2009, there was a widely publicized case of a Russian spy ring working in the United States. One of their tactics was simply to befriend key employees in target organizations and, through ongoing conversations, slowly elicit key data.

Another interesting way of using social engineering would be via email. In very large organizations, one cannot know every member. This loophole allows the clever industrial spy to send an email message claiming to come from some other department and perhaps simply asking for sensitive data. A corporate spy might, for example, forge an email to appear to be coming from the legal office of the target company requesting an executive summary of some research project.



FIGURE 7.4 Social engineering used as low-tech espionage.

Computer security expert Andrew Briney (Information Security, 2003) places people as the number-one issue in computer security.

Spyware Used in Industrial Espionage

Clearly, any software that can monitor activities on a computer can be used in industrial espionage. *Security IT World*, an online e-zine, featured an article in its October 2003 issue that dealt with the fact that monitoring a computer is an easy thing to do in the twenty-first century. The problem still persists to this day, with many security experts stating that spyware is at least as widespread as viruses. One method to accomplish monitoring is via spyware, which we discussed in detail in Chapter 5, “Malware.” Clearly, software or hardware that logs key strokes or takes screenshots would be most advantageous to the industrial spy.

The application of this type of software to espionage is obvious. A spy could get screenshots of sensitive documents, capture logon information for databases, or in fact capture a sensitive document as it is being typed. Any of these methods would give a spy unfettered access to all data that is processed on a machine that contains spyware.

Steganography Used in Industrial Espionage

Steganography is a different way of keeping messages secret. Rather than hide them through encryption, it protects communication via obscuring them. Messages are hidden within images. And in some cases other images are hidden within images. The word *steganography* comes from the Greek *steganos*, meaning covered or secret, and *graphy*, meaning writing or drawing. There are several technical means to accomplish this, but the most common is to conceal the data in the least significant bits of an image file. However, data can be concealed in any sort of digital file.

It should also be noted that historically there have been nontechnical means of hiding messages. A few notable examples include the following:

- The ancient Chinese wrapped notes in wax and swallowed them for transport.
- In ancient Greece a messenger’s head might be shaved, a message written on his head, and then his hair was allowed to grow back.
- In 1518, Johannes Trithmeus wrote a book on cryptography and described a technique where a message was hidden by having each letter taken as a word from a specific column.

You might think that steganography requires a great deal of technical knowledge to accomplish; however, there are many software packages available that will perform the steganography for you. Quick Stego and Invisible Secrets are two very easy-to-use software tools that will do steganography for you. MP3Stego is a free tool that hides data inside MP4 files. These are just a few of the tools that one can find on the Internet. The widespread availability of cheap or free tools that are easy to use makes steganography a greater threat to any organization.

Phone Taps and Bugs

Of course, there is always the possibility of using phone taps. A phone tap is simply the process of tying into the phone line at some point and intercepting calls. This is often done at some utility location inside the building one wishes to tap. Obviously, this sort of attack requires the attacker to enter on or near the premises, compromise phone equipment, and have the skill to tap into the phone line.

Protecting Against Industrial Espionage

By now, you are aware that there are many ways that your organization's valuable information assets can be compromised. The question thus becomes this: What steps can you take to alleviate the danger? Note that I said "alleviate" the danger. There is nothing you can do to make any system, any information, or any person totally secure. Totally unbreakable security is simply a myth. The best you can do is work to achieve a level of security that makes the effort required to get information more costly than the value of the information.

One obvious protection is to employ antispyware software. As was mentioned earlier in this book, many antivirus programs also have antispyware capabilities. This software, coupled with other security measures such as firewalls and intrusion detection software (both examined in Chapter 9, "Computer Security Technology"), should drastically reduce the chance that an outside party will compromise your organization's data. Furthermore, implementing organizational policies (also discussed in Chapter 9) that help guide employees on safely using computer and Internet resources will make your system relatively secure. If you add to your protection arsenal the strategy of encrypting all transmissions, your system will be as secure as you can reasonably make it. (Chapter 8, "Encryption, is devoted to encryption.) However, all of these techniques (firewalls, company policies, antispyware, encryption, and so forth) will only help in cases in which the employee is not the spy. What do you do to ameliorate the danger of employees intentionally stealing or compromising information? Actually, there are several courses of action any organization can take to lessen risks due to internal espionage. Here are 12 steps you can use:

1. Always use all reasonable network security: firewalls, intrusion detection software, antispyware, patching and updating the operating system, and proper usage policies.
2. Give the personnel of the company access to only the data that they absolutely need to perform their jobs. This concept is referred to as *least privileges*. The employees are given the minimum privileges necessary to perform their job tasks. Use a need-to-know approach. One does not want to stifle discussion or exchange of ideas, but sensitive data must be treated with great care.
3. If possible, set up a system for those employees with access to the most sensitive data in which there is a rotation or a separation of duties. In this way, no one employee has access and control over all critical data at one time.
4. Limit the number of portable storage media in the organization (such as CD burners, and flash drives) and control access to these media. Log every use of such media and what was stored.

Some organizations have even prohibited cell phones because many phones allow the user to photograph items and send the pictures electronically.

5. Do not allow employees to take documents/media home. Bringing materials home may indicate a very dedicated employee working on her own time or a corporate spy copying important documents and information.
6. Shred documents and melt old disks/tape backups/CDs. A resourceful spy can often find a great deal of information in the garbage. If any storage media is disposed of, it should be completely wiped. Degaussing is a good technique for hard drives and USB drives.
7. Do employee background checks. You must be able to trust your employees, and you can only do this with a thorough background check. Do not rely on “gut feelings.” Give particular attention to information technology (IT) personnel who will, by the nature of their jobs, have a greater access to a wider variety of data. This scrutiny is most important with positions such as database administrators, network administrators, and network security specialists.
8. When any employee leaves the company, scan the employee’s PC carefully. Look for signs that inappropriate data was kept on that machine. If you have any reason to suspect inappropriate usage, then store the machine for evidence in subsequent legal proceedings.
9. Keep all tape backups, sensitive documents, and other media under lock and key, with limited access to them.
10. If portable computers are used, then encrypt the hard drives. Encryption prevents a thief from extracting useable data from a stolen laptop. There are a number of products on the market that accomplish this encryption, including the following:
 - TrueCrypt (see Figure 7.5) is one example of a free tool for encrypting drives, folders, or partitions. The tool is remarkably easy to use and can be found at www.truecrypt.org/. There are several other similar tools; most are low cost or free.
 - Microsoft Windows includes two types of encryption. Windows 7 Enterprise or Ultimate edition includes BitLocker for encrypting entire hard drives. BitLocker is also available on later versions of Windows (8, 8.1, 10). And all versions of Windows since Windows 2000 have included Encrypted File System for encrypting specific files or folders (see Figure 7.6).
 - This list is not exhaustive; therefore, it is highly recommended that you carefully review a variety of encryption products before making a selection.
11. Have all employees with access to any sensitive information sign nondisclosure agreements. Such agreements give you, the employer, a recourse should an ex-employee divulge sensitive data. It is amazing how many employers do not bother with this rather simple protection.

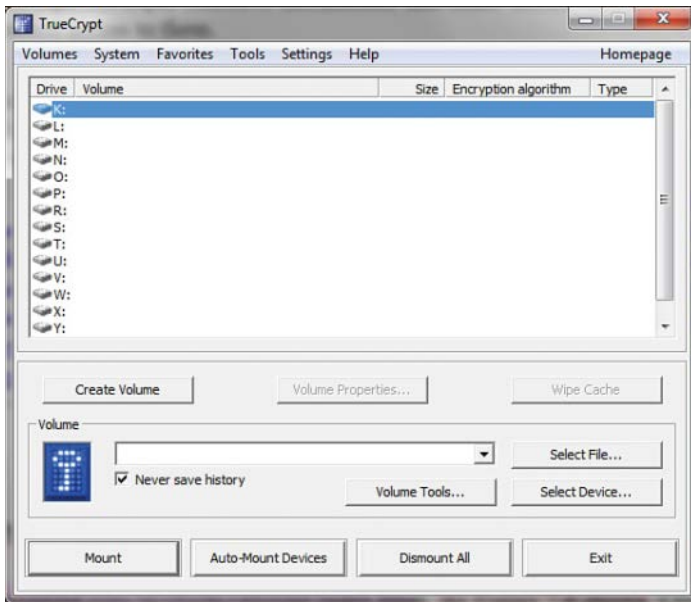


FIGURE 7.5 TrueCrypt.

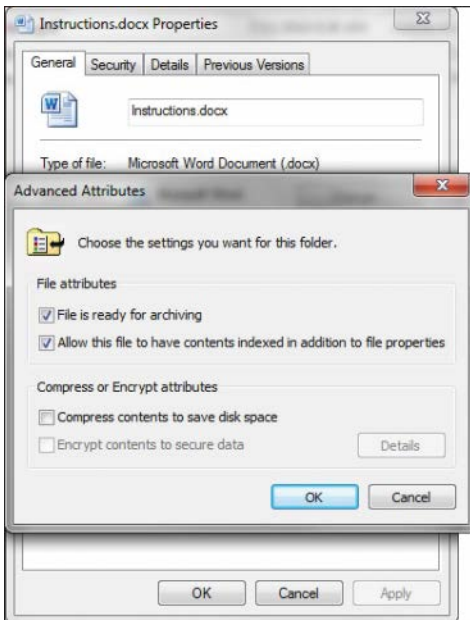


FIGURE 7.6 Windows EFS.

12. Have security awareness sessions. Clearly, employee education is one of the most important things you can do. An organization should have some method for routinely advising employees about security issues. An excellent way to do that is to have an intranet site that has security bulletins posted to it. It is also a good idea to have periodic training sessions for employees. These need not be lengthy or in depth. Most nontechnical employees only need an introduction to security concepts.

Unfortunately, following these simple rules will not make you totally immune to corporate espionage. However, using these strategies will make any such attempts much more difficult for any perpetrator; thus, you will improve your organization's data security.

Industrial Espionage Act

The Industrial Espionage Act of 1996 was the first U.S. law to criminalize theft of commercial trade secrets. This law provides for significant penalties for violators. Quoting from the actual law:¹

- (a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly—
- (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
 - (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
 - (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
 - (4) attempts to commit any offense described in paragraphs (1) through (3); or
 - (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

Spear Phishing

Phishing, as you know, is the process of attempting to get personal information from a target in order to steal the target's identity or compromise the target's system. A common technique is to send out a mass email that is designed to entice recipients into clicking on a link that purports to be some financial institution's website but is actually a phishing website.

1. http://fas.org/irp/congress/1996_rpt/s104359.htm

Spear phishing is using the same technology in a targeted manner. For example, if an attacker wanted to get into the servers at a defense contractor, he might craft email and phishing websites specifically to target software and network engineers at that company. The emails might be made to appear of interest to that specific subgroup of people. Or the attacker might even take the time to learn personal details of a few of these individuals and target them specifically. This technique has been used against executives at various companies. In 2010 and 2011, this problem began to grow significantly.

This has since been expanded even more into the process of whaling. *Whaling* attempts to compromise information regarding a specific, but highly valuable, employee. It uses the same phishing techniques, but highly customized to increase the chances that the single individual target will be fooled and actually respond to the phishing attempt.

Summary

A number of conclusions can be drawn from the examination of industrial espionage. The first conclusion: It does indeed occur. The case studies clearly demonstrate that industrial espionage is not some exotic fantasy dreamed up by paranoid security experts. It is an unfortunate, but quite real, aspect of modern business. If your firm's management chooses to ignore these dangers, then they do so at their own peril.

The second thing that can be concluded from this brief study of industrial espionage is that there are a variety of methods by which espionage can take place. An employee revealing confidential information is perhaps the most common. However, compromising information systems is another increasingly popular means of obtaining confidential and potentially valuable data. You will want to know the best way to protect your company and yourself. In the upcoming exercises at the end of this chapter, you will run screen-capture software, key loggers, and antispyware.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. What is the ultimate goal of espionage?
 - A. To subvert a rival government
 - B. To obtain information that has value
 - C. To subvert a rival business
 - D. To obtain information not otherwise available
2. What is the best outcome for a spy attempting an espionage activity?
 - A. To obtain information without the target even realizing he did so
 - B. To obtain information with or without the target realizing he did so
 - C. To obtain information and discredit the target
 - D. To obtain information and cause harm to the target
3. What is the usual motivating factor for corporate/industrial espionage?
 - A. Ideological
 - B. Political
 - C. Economic
 - D. Revenge

4. Which of the following types of information would be a likely target for industrial espionage?
 - A. A new algorithm that the company's IT department has generated
 - B. A new marketing plan that the company has formulated
 - C. A list of all the company's customers
 - D. All of the above
5. Which of the following is a likely reason that an organization might be reluctant to admit it has been a victim of corporate espionage?
 - A. It would embarrass the IT department.
 - B. It would embarrass the CEO.
 - C. It might cause stock value to decline.
 - D. It might lead to involvement in a criminal prosecution.
6. What is the difference between *corporate* and *industrial* espionage?
 - A. None; they are interchangeable terms.
 - B. Industrial espionage only refers to heavy industry, such as factories.
 - C. Corporate espionage only refers to executive activities.
 - D. Corporate espionage only refers to publicly traded companies.
7. You can calculate the value of information by what formula?
 - A. Resources needed to produce the information, plus resources gained from the information
 - B. Resources needed to produce the information, multiplied by resources gained from the information
 - C. Time taken to derive the information, plus money needed to derive the information
 - D. Time taken to derive the information, multiplied by money needed to derive the information
8. If a company purchases a high-end UNIX server to use for its research and development department, what is probably the most valuable part of the system?
 - A. The high-end UNIX server
 - B. The information on the server
 - C. The devices used to protect the server
 - D. The room to store the server

9. Information is an asset to your company if it
 - A. Cost any sum of money to produce
 - B. Cost a significant sum of money to produce
 - C. Might have economic value
 - D. Might cost significant money to reproduce
10. What is the greatest security risk to any company?
 - A. Disgruntled employees
 - B. Hackers
 - C. Industrial spies
 - D. Faulty network security
11. Which of the following is the best definition for *spyware*?
 - A. Software that assists in corporate espionage
 - B. Software that monitors activity on a computer
 - C. Software that logs computer keystrokes
 - D. Software that steals data
12. What is the highest level of security you can expect to obtain?
 - A. A level of security that makes the effort required to get information more than the value of the information
 - B. A level of security comparable with government security agencies, such as the Central Intelligence Agency
 - C. A level of security that has a 92.5% success rate in stopping intrusion
 - D. A level of security that has a 98.5% success rate in stopping intrusion
13. In the context of preventing industrial espionage, why might you wish to limit the number of company CD burners and control access to them in your organization?
 - A. An employee could use such media to take sensitive data out.
 - B. An employee could use such media to copy software from the company.
 - C. CDs could be a vehicle for spyware to get on your system.
 - D. CDs could be a vehicle for a virus to get on your system.

14. Why would you want to scan an employee's computer when he leaves the organization?
 - A. To check the work flow prior to leaving
 - B. To check for signs of corporate espionage
 - C. To check for illegal software
 - D. To check for pornography
15. What is the reason for encrypting hard drives on laptop computers?
 - A. To prevent a hacker from reading that data while you are online
 - B. To ensure that data transmissions are secure
 - C. To ensure that another user on that machine will not see sensitive data
 - D. To prevent a thief from getting data off of a stolen laptop

EXERCISES

EXERCISE 7.1: Learning About Industrial Espionage

1. Using the Web, library, journals, or other resources, look up a case of industrial or corporate espionage not already mentioned in this chapter.
2. Write a brief essay describing the facts in the case. The parties in the case and the criminal proceeding are of interest, but most of your discussion should focus on the technical aspects of the case. Be sure to explain how the espionage was conducted.

EXERCISE 7.2: Using Antispyware

Note that this exercise may be repeated with different antispyware products. It is a good idea for any person interested in computer security to be familiar with multiple antispyware products.

1. Go to the website of one of the antispyware utilities. (See Chapter 5 if you need more direction.)
2. Find instructions on the vendor's website.
3. Download the trial version of that software.
4. Install the software on your machine.
5. After installation, run the utility. What did it find? Record your results.
6. Let the utility remove or quarantine anything it found.

EXERCISE 7.3: Learning About Key Loggers

Note that this exercise may only be completed on machines where you have explicit permission to do so (no public computers).

1. Using any website, find and download a key logger. The following websites might help you locate a key logger:

www.kmint21.com/familykeylogger/
www.blazingtools.com/bpk.html

2. Install the key logger on your PC.
3. Examine how the key logger behaves on your machine. Do you notice anything that might indicate the presence of illicit software?
4. Run the antispyware software you downloaded in Exercise 2. Does the antispyware software detect the key logger?

EXERCISE 7.4: Screen-Capture Spyware

1. Using the Web, find and download a screen-capturing spyware application. The following website might be helpful to you in selecting an appropriate product. Warning: Since you are downloading spyware, it is likely that your system's antivirus/antispyware will give you a warning on some of these sites:

<http://en.softonic.com/s/screen-capture-spy-software>

2. Install and configure the application on your computer.
3. Run the application and note what it finds.
4. Run the antispyware from Exercise 2 and see whether it detects your spyware program.

EXERCISE 7.5: Learning About Hardware-Based Key Loggers

In this chapter, as well as in Chapter 5, we discussed software-based key loggers. However, there are also hardware-based key loggers.

1. Use the Internet to learn more about hardware-based key loggers. (You may wish to search for "Keycatcher" as a starting point.)
2. Write an essay outlining the way in which these key loggers work and how they could be implemented for either security or industrial espionage.

PROJECTS

PROJECT 7.1: Preventing Corporate Espionage

Using one of the websites listed in this book (you can also choose from the preferred resources in Chapter 1) or other resources, find a set of guidelines on general computer security. Write a brief essay comparing and contrasting those guidelines against the ones given in this chapter. Keep in mind that the guidelines in this chapter relate specifically to corporate espionage and not to general computer security.

PROJECT 7.2: Handling Employees

Write a brief essay describing steps regarding the handling of employees. Include all steps that you believe an organization should take to prevent corporate espionage. It is important that you support your opinions with sources and reasons.

If possible, visit a company and talk with someone in either the IT or personnel departments to determine how that company handles issues such as employee termination, rotation of duties, control of access to data, and so forth. Compare and contrast your steps to those used by the company you visited.

PROJECT 7.3: Asset Identification in Your Organization

Using the Asset Identification table found in this chapter or a similar table of your own design, identify the most valuable data in your organization (school or business) and what parties would most likely wish to access that data. Then write a brief guideline on how you might go about securing that data. In this project, you should tailor your security recommendations to the specific type of data you are trying to protect and against the most likely perpetrators of industrial espionage.

Case Study

David Doe is a network administrator for the ABC Company. David is passed over for promotion three times. He is quite vocal in his dissatisfaction with this situation. In fact, he begins to express negative opinions about the organization in general. Eventually, David quits and begins his own consulting business. Six months after David's departure, it is discovered that a good deal of the ABC Company's research has suddenly been duplicated by a competitor. Executives at ABC suspect that David Doe has done some consulting work for this competitor and may have passed on sensitive data. However, in the interim since David left, his computer has been formatted and reassigned to another person. ABC has no evidence that David Doe did anything wrong.

What steps might have been taken to detect David's alleged industrial espionage? What steps might have been taken to prevent his perpetrating such an offense?

This page intentionally left blank

A

access control policies, 263-264

AccessData FTK

Forensics Toolkit, 363

Imager, 356-358

ACK (ACKnowledge) bits, 41

active code scanning, virus scanners, 223

active IDS, 230

active scanning techniques, hacking

enumeration, 142-144

port scanning, 139-142

vulnerability assessment, 142

activities, IDS, 231

Address Resolution Protocol (ARP), 291

addresses (IP), 34, 41

CIDR (classless interdomain routing), 37-39

IPv4, 35-37

IPv6, 38-39

loopback addresses, 36

NAT (network address translation), 37

packets, 40

private, 36

public, 37

subnetting, 37

URLs (uniform resource locators), 39-40

addresses (MAC), 49-50

AddRoundKey step (AES), 198

Adlema, Len, 202

advance-fee scam, 59

Advanced Encryption Standard (AES), 197-199

Blowfish, 199

cipher-block chaining, 200

electronic codebook, 200

math, 199

RC4, 199

Serpent, 199

Skipjack, 200

advanced persistent threats (APTs), 126, 312

Advanced Research Projects Agency (ARPA), 41

AFCC (Air Force Cyber Command), 311

age, passwords, 283

Agent.btz worm, 311

Agnitum firewalls, 227

AHs (Authentication Headers), IPsec, 243

Air Force Cyber Command (AFCC), 311

alerts, IDS, 231

algorithms, 193

Atbash cipher, 189

binary operations, 192-193

Caesar cipher, 188

Enigma machine, 191-192

hashing, 207-208

multi-alphabet substitution, 189-190

PGP (Pretty Good Privacy), 205-206

public key, 201-205

rail fence cipher, 190-191

single-key encryption, 194

AES, 197-200

DES (Data Encryption Standard), 194-196

triple DES, 197

Allen, James, 67

analyzers, IDS, 230

AND operation, 192

Android, computer forensics, 377-378

Anonymous DDoS attacks, 98

antispyware, 172, 228-229

antivirus software, 221-224, 250

application gateway, firewalls, 226

Application log (Windows), 365

applications, patching, 277

Applications and Services log (Windows), 365

APTs (advanced persistent threats), 126, 312

armored viruses, 110

ARP (Address Resolution Protocol), 291

ARPA (Advanced Research Projects Agency), 41

ARPANET, 41

AS (authentication server), Kerberos, 238

Assange, Julian, 99

assessing systems, 277

firewalls, 281-282

IDS, 281-282

patches, 277-278

physical, 284-285

policies, 282-284

ports, 278-281

probing, 284

asset identification, 163

asymmetric cryptography, 185

asymmetric encryption, 201

Diffie-Hellman, 204-205

digital signatures, 207

Elliptic Curve, 205

fraudulent methods, 206-207

PGP (Pretty Good Privacy), 205-206

RSA, 202-204

Atbash cipher, 189

attachments, email, 255

scanning, virus scanners, 222

attack phase (NIST 800-115 security assessment), 151

attacks

advanced persistent threats (APTs), 126

assessing likelihood, 14-15

brute force, 188

buffer-overflow, 119-121

chosen plaintext, 213

ciphertext-only, 213

cross-site scripting, 146

DNS poisoning, 6, 13

DoS (denial of service), 6-9, 86-89

DDoS, 97-99

defending against, 99-100

ICMP flood attacks, 96

land attack, 97

LOIC (low orbit ion cannon), 89

ping of death (PoD), 96

security policies, 262

Smurf IP attack, 94-95

Stacheldraht tool, 91

TCP SYN flood attack, 91-94

teardrop attack, 96

TFN (Tribal Flood Network), 90-91

UDP flood attacks, 96

weaknesses, 91

XOIC, 89-90

economic, 315-317

general, 318

hacking, 338

security policies, 262-263

identifying, 6

identity theft, 338

increase, 3-4

insider threats, 6, 11-12

known plaintext, 212

logic bombs, 125-126

malicious web-based code, 125

malware

logic bombs, 7

login as system, 150

net user script, 149-150

pass the hash, 149

spyware, 7

TeraBIT virus maker, 148-149

Trojan horses, 7

viruses, 6

military operations, 317-318

new, 13-14

password cracking, 146-148

related-key, 213

rootkits, 124

security breaches, 6-8

session hijacking, 6, 11

social engineering, 170

spam, 126

spear phishing, 175-176

spyware

detection and elimination, 127-129

legal uses, 121

obtaining, 122-123

target delivery, 122

SQL script injection, 144-146

Trojan horses, 116-118

viruses

armored, 110

avoiding, 115-116

Bagle, 114

CryptoLocker, 111

CryptoWall, 112

detection and elimination, 127-129

FakeAV, 112

- Flame, 115
- Gameover Zeus, 111
- MacDefender, 112
- macro, 110
- memory-resident, 110
- Mimail, 114
- Morris worm, 115
- multi-partite, 110
- MyDoom, 116
- nonvirus, 114-115
- polymorphic, 111
- propagation, 109-110
- Rombertik, 111
- Sobig, 113-114
- sparse infector, 110
- Troj/Invo-Zip, 112
- virus scanners, 116
- W32/Netsky-P, 112
- web, 6, 9
 - cross-site scripting, 10-11
 - SQL injection, 9-10
- auctions, fraudulent, 62-63**
- auditing, 17**
- audit monitors, cloud, 384**
- authentication, 17, 236-238**
- Authentication Headers (AHs), IPsec, 243**
- authentication server (AS), Kerberos, 238**
- Autostart locations, Windows Registry, 374**
- AVG AntiVirus, 224**
- AVG virus scanner, 116**
- Aykroyd, Dan, 16**

B

- Back Orifice Trojan horse, 117**
- backbones, 34**
- background checks, 338**
 - civil court records, 344
 - employees, 173
 - prospective employees, general searches, 339-342
 - respecting privacy, 342
 - sex offender registries, 342-344
 - state court records, 345
 - Usenet, 346-347
- backup media, handling old, 288-289**
- backups, types, 267**
- Bagle virus, 114**
- bandwidth, 30**
- BCP (business continuity plan), 266**
- Bellaso, Giovan Battista, 190**
- Berners-Lee, Tim, 42**
- BIA (business impact analysis), 266-267**
- bid shielding, auctions, 63**
- bid siphoning, auctions, 63**
- binary operations, 192-193**
- BitLocker, 173**
- black hat hacking, 15**
 - reconnaissance phase, 137
 - active scanning, 139-144
 - passive scanning, 137-138
- BlackEnergy malware, 315**
- block ciphers, 194**
- blocking ICMP packets, 99**
- Bloomberg, Inc., industrial espionage, 167**
- Bloomberg, Michael, 167**
- Blowfish block cypher, 199**
- Bogachev, Evgeniy, 111**
- Bosselaers, Antoon, 208**
- botnets, 97, 111**

breaches, system administration policies, 261

Briney, Andrew, 171

browsers

finding evidence in, 364

secure settings, 74-78

brute force attacks, 188

buffer-overflow attacks, 119-120

Sasser virus, 120-121

buffers, 119

bugs, industrial espionage, 172

business continuity plan (BCP), 266

business impact analysis (BIA), 266-267

BYOD (bring your own device), security policies, 256-257

C

CA (certificate authority), 239

cables, 29-30

Caesar cipher, 188

Cain and Abel enumeration tool, 143-144

carriers, steganography, 210

CASP (Certified Advanced Security Practitioner), 5

Category 6 cable, 30

CBC (cipher-block chaining), 200

cell phone forensics, 375-378

Cellebrite tool, 364

CENTCOM (Central Command), 311

Center for Internet Security, 285

Central Command (CENTCOM), 311

Cerf, Vince, 41

CERT (Computer Emergency Response Team), 21, 115

Information Assurance in Small Organization workbook, 163-165

certificate authority (CA), 239

certificates, digital, 238

X.509, 239-240

certification

CASP (Certified Advanced Security Practitioner), 5

Certified Cyber Forensics Professionals, 300

Certified Ethical Hacker, 300

Certified Forensics Analyst (GCFA), 381

Certified Forensics Examiner (GCFE), 381

Certified Hacking Investigator, 300

CISSP (Certified Information System's Security Professional), 5

CNE (Certified Novel Engineer), 299

computer forensics, 380-381

IT (information technology), 299-300

penetration testing, 136

Security+, 5

chain of custody, computer forensics, 360

Challenge Handshake Authentication Protocol (CHAP), 236

Chang, Jeremy, 166

change requests, system administration policies, 259-261

channel, steganography, 210

CHAP (Challenge Handshake Authentication Protocol), 236

checklists, policies, 283

children, cyber stalking, 70-71

China Eagle Union, 312

Chinese Military, APTs, 126

chosen plaintext attacks, 213

Christenson, Kai, 68

CIA triangle, 18

CIDR (classless interdomain routing), 37-39

cipher-block chaining (CBC), 200

cipher text, encryption, 193

ciphertext-only attacks, 213

CISA (Certified Information Systems Auditor), 5

Cisco Systems

certifications, 299

firewalls, 227

CISSP (Certified Information System's Security Professional), 5, 300

Citrix firewalls, 282

civil court record searches, 344

classes, networks, 35

classification, data, 265

classless interdomain routing (CIDR), 37-39

client errors, 39

cloud forensics, 384

CNE (Certified Novel Engineer), 299

commands

Fc, 370

ipconfig, 43

net sessions, 369

Netcat, 356

netstat, 46

Netstat, 370

nslookup, 47

Openfiles, 369

ping, 39, 45, 87-88

Snort, 234

SQL, 9

tracert, 45-46

tracert, 45-46

WhoIS, 33

Computer Crime Acts, 20

Computer Emergency Response Team (CERT), 21, 115

computer forensics, 354-355

cell phone, 375-378

certification, 380-381

chain of custody, 360

documentation, 359

EU guidelines, 362

expert witnesses, 381-382

FBI guidelines, 360-361

finding evidence in browser, 364

finding evidence in system logs, 365-366

handling suspect drive, 355-356

imaging drive, 356-358

live machines, 358-359

Locard's principle of transference, 363

network, 382

operating system utilities, 369-370

retrieving deleted files, 366-369

securing evidence, 359

SWGDE (Scientific Working Group on Digital Evidence), 362-363

tools, 363-364

U.S. Secret Service guidelines, 361-362

virtualization, 382-384

Windows Registry, 371-374

Computer Security Act of 1987, 20

Computer Security Institute survey, 14

computer systems. See system security

configuration

desktop, security policies, 256

firewalls, 226-227

Internet Explorer, 74-78

connect scans (Nmap), 140

connection speeds, Internet, 32

cookies, 7

- RST, 93
- spyware, 121
- SYN, 92-93

co-prime numbers, 202**corporate espionage. See industrial espionage****costs, cybercrime, 3****Counterpane Internet Security, 324****Cox, William, 68****crackers, 137****cracking, 7****credibility, cyber stalking, 69****CRL (certificate revocation list), 240****cross-site scripting, 10-11, 146****cryptanalysis, 211-213****cryptography, 184**

- asymmetric, 185
- cryptanalysis, 211-213
- decryption, 185
- distinguishing algorithm, 212
- encryption, 185-187
 - AES, 197-200
 - Atbash cipher, 189
 - binary operations, 192-193
 - Caesar cipher, 188
 - cipher text, 193
 - digital signatures, 207
 - Enigma machine, 191-192
 - fraudulent methods, 206-207
 - hashing, 207-208
 - keys, 193
 - MAC (Message Authentication Code), 208-209
 - multi-alphabet substitution, 189-190
 - PGP (Pretty Good Privacy), 205-206
 - plain text, 193

- public key, 201-205
- rail fence cipher, 190-191
- rainbow tables, 209-210
- single-key, 194-196
- steganography, 210-211
- triple DES, 197
- global deduction, 212
- information deduction, 212
- instance deduction, 212
- Internet, 213
- steganography, 210-211
- symmetric, 185
- total breaks, 212

Cryptography.org, 187**CryptoLocker virus, 111****CryptoWall virus, 112****CSNET, 42****cyber stalking, 65-68, 79**

- crimes against children, 70-71
- evaluating, 69-70

cyber terrorism, 310, 322-326

- Agent.btz worm, 311
- APT (Advanced Persistent Threat), 312
- China Eagle Union, 312
- Dark Web, 331-332
- defending against, 329-330
- economic attacks, 315-317
- future trends, 326-329
- general attacks, 318
- India/Pakistan, 313
- information warfare, 319-322
- military operations attacks, 317-318
- recruiting, 330
- Russia, 313
- SCADA (Supervisory Control and Data Acquisitions), 318
- TOR (The Onion Router), 330-331
- weapons, 313-315

cyber warfare

- economic attacks, 315-317
- general attacks, 318
- military operations attacks, 317-318
- SCADA (Supervisory Control and Data Acquisitions), 318
- weapons, 313-315

cybercrime. See attacks**Cybersecurity Research and Education Act of 2002, 326-327****Cyberterrorism Preparedness Act of 2002, 326-327**

D**Daemen, Joan, 197****DAM (database activity monitoring), 235****DAMP (database activity monitoring and prevention), 235****Dark Web, 331-332****DARPA (Defense Advanced Research Projects Agency), 41****data classification, 265****Data Encryption Standard (DES), 194-196****data partitions, iOS, 377****data sources, IDS, 231****data transmission, networks, 32-34****databases, 235**

- relational, SQL script injection, 144-146

Daubert standard, expert witnesses, 382**DBMS (database management system), 235****DDoS (distributed denial of service) attacks, 97**

- defending against, 99-100
- MyDoom, 97-99

decryption, 185**DefCon convention, war-driving contest, 8****Defense Advanced Research Projects Agency (DARPA), 41****deleted files, retrieving, 366-369****demilitarized zone (DMZ), 289-290****denial of service (DoS) attacks. See DoS (denial of service) attacks****departing employees, system administration policies, 258-259****DES (Data Encryption Standard), 194-196****desktop configuration, security policies, 256****developmental policies, 264****differential backups, 267****Diffie, Whitfield, 204****Diffie-Hellman encryption, 204-205****digital certificates, 238-240****digital forensics. See computer forensics****digital signatures, 207**

- PGP (Pretty Good Privacy), 239

disaster recovery plan (DRP), 266**disaster recovery policies, 266-268****discovery phase (NIST 800-115 security assessment), 151****disinformation, 322****DiskDigger, retrieving deleted files, 366-369****disks, RAID levels, 268****distinguished names, X.509 certificates, 239****distributed denial of service (DDoS). See DDoS (distributed denial of service) attacks****DMZ (demilitarized zone), 289-290****DNS (Domain Name Service), 33, 42****DNS poisoning, 6, 13****Dobbertin, Hans, 208****documentation, computer forensics, 359**

documents, shredding, 173

DOD attacks, clearances, 265

Domain Name Service (DNS), 33, 42

doomjuice virus, 116

DoS (denial of service) attacks, 6-9, S86

DDoS, 88, 97-99

defending against, 99-100

land, 97

LOIC (low orbit ion cannon), 89

ping of death (PoD), 96

security policies, 262

Smurf IP, 94-95

Stacheldraht tool, 91

TCP SYN flood, 91-94

teardrop, 96

TFN (Tribal Flood Network), 90-91

UDP flood, 96

weaknesses, 91

XOIC, 89-90

download scanning, virus scanners, 222

doxing, 13

drives

handling for forensics, 355-356

imaging, 356-358

DRP (disaster recovery plan), 266

dual-homed host firewalls, 226

Duronio, Roger, 125

E

EAP (Extensible Authentication Protocol), 237

Easttom, Chuck, contact information, 342

corollary, 206

**EC Council, penetration testing
certifications, 136**

ECB (electronic codebook), 200

economic attacks, 315-317

**economic espionage. See industrial
espionage**

**EDGE (Enhanced Data Rates for GSM
Evolution), 376**

Edwards, John, 326

EFS (Encrypted File System), 173-175

electronic codebook (ECB), 200

eLiTeWrap, 118

EliteWrapper, 117

Elliptic Curve encryption, 205

Ellison, Larry, 168

email

scanning, 222

security policies, 254-255

employees

access control policies, 263-264

background checks, 173, 338

civil court records, 344

general searches, 339-342

respecting privacy, 342

sex offender registries, 342-344

state court records, 345

Usenet, 346-347

developmental policies, 264

disaster recovery policies, 266-268

nondisclosure and noncompete agreements, 162

security policies, 251, 258

BYOD (bring your own device), 256-257

desktop configuration, 256

email usage, 254-255

installing/uninstalling software, 255

instant messaging, 255-256

Internet usage, 253-254

passwords, 252-253

- system administration policies, 258
 - change requests, 259-261
 - departing employees, 258-259
 - new employees, 258

Encapsulating Security Payloads (ESPs), IPsec, 243

EnCase tool, 364

Encrypted File System, 173-175

encryption, 184-187

- asymmetric, 185
- Atbash cipher, 189
- binary operations, 192-193
- Caesar cipher, 188
- cipher text, 193
- cryptanalysis, 211-213
- digital signatures, 207
- Enigma machine, 191-192
- fraudulent methods, 206-207
- hashing, 207-208
- Internet, 213
- key schedules, 195
- keys, 193
- MAC (Message Authentication Code), 208-209
- multi-alphabet substitution, 189-190
- PGP (Pretty Good Privacy), 205-206
- plain text, 193
- public key, 201
 - Diffie-Hellman, 204-205
 - Elliptic Curve, 205
 - RSA, 202-204
- rail fence cipher, 190-191
- rainbow tables, 209-210
- single-key, 194
 - AES (Advanced Encryption Standard), 197-200
 - DES (Data Encryption Standard), 194-196
 - triple DES, 197
- symmetric, 185

Enhanced Data Rates for GSM Evolution (EDGE), 376

Enigma machine, 191-192

enumeration, 142-144

Error 404: File Not Found, 39

espionage, industrial, 160-162

- Bloomberg, Inc., 167
- FBAR technology, 165
- General Motors, 166
- Houston Astros, 165
- Industrial Espionage Act, 175
- information as asset, 162-165
- Interactive Television Technologies, Inc., 167
- low-tech, 168-171
- phone taps and bugs, 172
- protecting against, 172-175
- spear phishing, 175-176
- spyware, 171
- steganography, 171
- trends, 167-168
- VIA Technology, 166

ESPs (Encapsulating Security Payloads), IPsec, 243

ethical hacking, 16

EU guidelines, computer forensics, 362

Euhler's totient, 202-203

events, IDS, 231

evidence, 361

evidence, securing, 359

exit interviews, 162

expert witnesses, computer forensics, 381-382

Extensible Authentication Protocol (EAP), 237

F

Facebook

- background checks, 340
- productivity, 258

FakeAV virus, 112

false negatives, virus scanners, 223

false positives, virus scanners, 222-223

Fannie Mae, logic bomb attack, 126

FastMail, DDoS attacks, 99

fault tolerance, 267-268

FBAR technology, industrial espionage, 165

FBI guidelines, computer forensics, 360-361

FBI state registry of sex offenders, 342-344

Fc command, 370

federal rule 702, expert witnesses, 381

Feistel ciphers, 194

file scanning, virus scanners, 222

File Transfer Protocol (FTP), 33

files, retrieving deleted, 366-369

FIN (FINish) bits, 41

FIN scans (Nmap), 140

FinFisher spyware, 314

firewalls, 17, 48, 172

- application gateway, 226
- choosing, 281-282
- commercial, 227-228
- configurations, 226-227
- limitations, 224
- logs, 228
- packet filtering, 225
- stateful packet inspection, 225

Flame virus, 115, 314

footprinting, 316

forensics, 354-355

- cell phone, 375-379
- certification, 380-381
- chain of custody, 360
- documentation, 359
- EU guidelines, 362
- expert witnesses, 381-382
- FBI guidelines, 360-361
- finding evidence in browser and system logs, 364-366
- handling suspect drive, 355-356
- imaging drive, 356-358
- live machines, 358-359
- Locard's principle of transference, 363
- network, 382
- operating system utilities, 369-370
- retrieving deleted files, 366-369
- securing evidence, 359
- SWGDE (Scientific Working Group on Digital Evidence), 362-363
- tools, 363-364
- U.S. Secret Service guidelines, 361-362
- virtualization, 382-384
- Windows Registry, 371-374

Forensics Toolkit (FTK), 363

ForwardedEvents log (Windows), 365

fraud, 58-59, 79

- auction, 62-63
- identity theft, 63-64
 - phishing, 65
 - protecting against, 73
- investment offers
 - advice, 60-61
 - Nigerian advance-fee scam, 59
 - protecting against, 72
- laws against, 72

frequency analysis, cryptanalysis, 212

frequency, cyber stalking, 69

F-Secure website, 21

FTK (Forensics Toolkit), 363

Imager, 356-358

FTP (File Transfer Protocol), 33

full backup, 267

G

GameOver ZeuS virus, 111

GCFE (Certified Forensics Examiner), 381

General Motors, industrial espionage, 166

GIAC (Global Information Assurance Certification), 300

global deduction, cryptography, 212

Global System for Mobile Communications (GSM), 376

GM (General Motors), industrial espionage, 166

Gonzalez, Amy, 68

gray hat hackers, 15, 137

guidelines, security policies, 264

H

hackers, 338

black hat, 15, 137

Certified Ethical Hacker certification, 300

gray hat, 15, 137

hacktivists, 323

Jack, Barnaby, 14

Mitnick, Kevin, 8

script kiddies, 16, 137

skillful, 4-5

slang, 15

white hat, 15, 137

hacking, 6-8, 338

cross-site scripting, 146

ethical, 16

industrial espionage, 160-162

Bloomberg, Inc., 167

FBAR technology, 165

General Motors, 166

Houston Astros, 165

Industrial Espionage Act, 175

information as asset, 162-165

Interactive Television Technologies, Inc., 167

low-tech, 168-171

phone taps and bugs, 172

protecting against, 172-175

spear phishing, 175-176

spyware, 171

steganography, 171

trends, 167-168

VIA Technology, 166

malware, 148

login as system, 150

net user script, 149-150

pass the hash, 149

TeraBIT virus maker, 148-149

password cracking, 148

penetration testing, 151-153

phreaking, 16-17, 137

reconnaissance phase

active scanning, 139-144

passive scanning, 137-138

security policies, 262-263

social engineering, 8

SQL script injection, 144-146

war-driving, 8

white hat, 136

hacktivists, 323

half-open scans (SYN), 140

Hao Zhang, 165

harassment, 67

hardening computer systems, 286

hash values, 93

hashing, 93, 207-208

headers, packets, 40

Hebert's cryptography website, 187

Hellman, Martin, 204, 209

heuristic scanning, virus scanners, 222

HIPAA (Health Insurance Portability and Accountability Act), 269

history, passwords, 283

hives, Windows Registry, 371-372

honey pots, 235-236

hosts, 41

Houston Astros, industrial espionage, 165

HTML (Hypertext Markup Language), 42

HTTP (Hypertext Transfer Protocol), 33, 42

HTTPS (Hypertext Transfer Protocol Secure), 33

hubs, networks, 31

Hutchinson, Shawn Michael, 67

hypervisors, cloud, 384

I

ICCI (integrated circuit card identification), 375

ICMP (Internet Control Message Protocol), 33
 packets, 94
 blocking, 99

iDEN (integrated Digitally Enhanced Network), 376-377

identifying threats, 6

identity theft, 63-64, 79, 338

 laws against, 72

 phishing, 65

 protecting against, 73

IDS (intrusion detection system), 17, 229, 281-282

 active, 230

 activities, 231

 alerts, 231

 analyzers, 230

 DAM (database activity monitoring), 235

 data sources, 231

 events, 231

 honey pots, 235

 intrusion identification, 230

 managers, 230

 notification, 231

 operators, 230

 passive, 229

 sensors, 230

 Snort, 231-235

IETF (Internet Engineering Task Force), 42

IKE (Internet key exchange), IPsec, 243

IMEI (International Mobile Equipment Identity), 375

Imitation Game, The, 192

IMSI (international mobile subscriber identity), 375

incremental backups, 267

industrial espionage, 160-162

 Bloomberg, Inc., 167

 FBAR technology, 165

 General Motors, 166

 Houston Astros, 165

 Industrial Espionage Act, 175

 information as asset, 162-165

 Interactive Television Technologies, Inc., 167

- low-tech, 168-171
- phone taps and bugs, 172
- protecting against, 172-175
- spear phishing, 175-176
- spyware, 171
- steganography, 171
- trends, 167-168
- VIA Technology, 166
- Industrial Espionage Act of 1996, 175**
- Infobel, 341**
- Information Assurance in Small Organization workbook (CERT), 163-165**
- information deduction, cryptography, 212**
- Information Systems Security Architecture Professional (ISSAP), 300**
- Information Systems Security Engineering Professional (ISSEP), 300**
- Information Systems Security Management Professional (ISSMP), 300**
- information warfare, 319-326**
- insider threats, 6, 11-12**
- installing software, security policies, 255**
- instance deduction, cryptography, 212**
- instant messaging, security policies, 255-256**
- integrated circuit card identification (ICCI), 375**
- integrated Digitally Enhanced Network (iDEN), 376-377**
- intensity, cyber stalking, 70**
- Interactive Television Technologies, Inc., industrial espionage, 167**
- International Mobile Equipment Identity (IMEI), 375**
- Internet**
 - connection speeds, 32
 - cryptography, 213
 - establishment of, 41
 - expansion, 3
 - IP addresses, 34-41
 - ISPs (Internet service providers), 34
 - security policies, 253-254
- Internet Control Message Protocol (ICMP). See ICMP (Internet Control Message Protocol)**
- Internet Engineering Task Force (IETF), 42**
- Internet Explorer, secure settings, 74-78**
- Internet fraud. See fraud**
- Internet key exchange (IKE), IPsec, 243**
- Internet Relay Chat (IRC), 33**
- Internet Security Association and Key Management Protocol (ISAKMP), 243**
- Internet service providers (ISPs), 34**
- intrusion deflection, 235-236**
- intrusion detection system (IDS). See IDS (intrusion detection system)**
- intrusion deterrence, 236**
- investment offers, fraudulent, 59-61, 72**
- Invisible Secrets, 171, 211**
- iOS computer forensics, 377**
- IP addresses**
 - CIDR (classless interdomain routing), 37-39
 - IPv4, 35-37
 - IPv6, 38-39
 - loopback addresses, 36
 - NAT (network address translation), 37
 - packets, 40
 - private, 36
 - public, 37
 - subnetting, 37
 - URLs (uniform resource locators), 39-40
- ipconfig command, 43**
- IPsec, 243-244**
- IRA (Irish Republican Army), 319**

IRC (Internet Relay Chat), 33

Irish Republican Army (IRA), 319

ISAKMP (Internet Security Association and Key Management Protocol), 243

ISPs (Internet service providers), 34

ISSAP (Information Systems Security Architecture Professional), 300

ISSEP (Information Systems Security Engineering Professional), 300

ISSMP (Information Systems Security Management Professional), 300

issuer, X.509 certificates, 239

J

Jack, Barnaby, 14

Johnson, Jeffery, 14

Kane, Heather, 68

Kaspersky antivirus software, 224

Kaspersky virus scanner, 116

KDC (key distribution center), Kerberos, 238

Kerberos, 237-238

Kerckhoff, Auguste, 206

Kerckhoff's principle, 206

key distribution center (KDC), Kerberos, 238

key loggers, 7

key schedules, 195

key space, 188

keyed cryptographic hash function, 209

keys, encryption, 193

Knight, Scott, 68

known plaintext attacks, 212

Koblitz, Neil, 205

L

L2TP (Layer 2 Tunneling Protocol), 243

land attacks, 97

Lauffenburger, Michael, 125

laws against fraud, 72

Layer 2 Tunneling Protocol (L2TP), 243

layered security approach, 18

LEAP (Lightweight Extensible Authentication Protocol), 237

least privileges, 18, 172

letter frequency distribution, 188

Lightweight Extensible Authentication Protocol (LEAP), 237

LinkedIn, background checks, 340

Linux logs, finding evidence in, 366

listing USB devices, 373

live machines, conducting forensics, 358-359

local deduction, cryptography, 212

local networks, 29-31

Locard, Edmond, 363

Locard's principle of transference, 363

logic bombs, 7, 125-126

logical network perimeter, cloud, 384

login as system attacks, 150

logs

 firewalls, 228

 routers, 291

 system, finding evidence in, 365-366

LOIC (low orbit ion cannon), 8, 89

Long Term Evolution (LTE), 376

loopback addresses, 36

Lopez, Inaki, 166

Low Earth Orbit Ion Cannon tool, 16
low orbit ion cannon (LOIC), 8, 89
low-tech industrial espionage, 168-171
LsaLogonUser, 149
LTE (Long Term Evolution), 376
Luhnnow, Jeff, 165

M

MAC (Message Authentication Code), 208-209
MAC addresses, 49-50
MacDefender virus, 112
macro viruses, 110
Makwana, Rajendrasinh, 126
malicious web-based code, 125
malware, 6, 148

- advanced persistent threats (APTs), 126
- BlackEnergy, 315
- buffer-overflow attacks, 119-121
- cyber warfare, 313
- FinFisher, 314
- Flame, 314
- logic bombs, 7, 125-126
- login as system, 150
- malicious web-based code, 125
- net user script, 149-150
- NSA ANT Catalog, 315
- pass the hash, 149
- rootkits, 124
- spam, 126
- spyware, 7, 121
 - detection and elimination, 127-129
 - industrial espionage, 171
 - legal uses, 121
 - obtaining, 122-123
 - target delivery, 122

StopGeorgia.ru, 314
Stuxnet, 313-314
TeraBIT virus maker, 148-149
Trojan horses, 7, 116-118
viruses, 6, 109-111

- armored, 110
- avoiding, 115-116
- Bagle, 114
- CryptoLocker, 111
- CryptoWall, 112
- detection and elimination, 127-129
- FakeAV, 112
- Flame, 115
- GameOver Zeus, 111
- MacDefender, 112
- macro, 110
- memory-resident, 110
- Mimail, 114
- Morris worm, 115
- multi-partite, 110
- MyDoom, 116
- nonvirus, 114-115
- polymorphic, 111
- propagation, 109-110
- Rombertik, 111
- Sobig, 113-114
- sparse infector, 110
- Troj/Invo-Zip, 112
- virus scanners, 116
- W32/Netsky-P, 112

Malwarebytes antivirus software, 224

managers, IDS, 230

Matusiewicz, David, 68

Matusiewicz, Lenore, 68

maximum tolerable downtime (MTD), 267

MBSA (Microsoft Baseline Security Analyzer), 291-293

McAfee

- antivirus software, 224
- Personal Firewall, 281
- virus scanner, 116

MCITP (Microsoft Certified Information Technology Professional), 299

MD5 encryption, 208

mean time to repair (MTTR), 267

Medico, Joseph, 67

memory-resident viruses, 110

Message Authentication Code (MAC), 208-209

micro blocks, TCP SYN flood attack, 92

microdots, 211

Microsoft Baseline Security Analyzer (MBSA), 291-293

Microsoft Outlook viruses, 109

Microsoft Security Advisor website, 21

military operations attacks, 317-318

Miller, Victor, 205

Mimail virus, 114

Mitnick, Kevin, 8

MixColumns step (AES), 198

mobile malicious code, 125

modulus operations, 202-203

mono-alphabet substitution method, 188

Morris, Robert Tappan, 11, 115

Mosaic browser, 42

MP3Stego, 171, 211

MS Exchange templates, 285

MTD (maximum tolerable downtime), 267

MTTR (mean time to repair), 267

multi-alphabet substitution, 189-190

multi-partite viruses, 110

Murphy, Robert James, 66

MyDoom attacks, 97-99, 116, 311

N

NAPs (network access points), 34

National Center for State Courts, 345

National Security Agency (NSA). See NSA (National Security Agency)

NAT (network address translation), 37

Nessus vulnerability scanner, 293-298

net sessions command, 369

net user script, 149-150

NetBIOS, 33

netcat command, 356

netstat command, 46, 370

network access points (NAPs), 34

network address translation (NAT), 37

network administrators, background checks, 339

network host-based firewalls, 226

network interface cards (NICs), 29

Network News Transfer Protocol (NNTP), 33

network utilities, 42

- ipconfig, 43
- netstat, 46
- nslookup, 47
- ping, 45
- tracert, 45-46

networks, 29

- backbones, 34
- cellular, computer forensics, 376-377
- classes, 35
- data transmission, 32-34
- DMZ (demilitarized zone), 289-290
- firewalls, 48, 224-228

- forensics, 382
- Internet connection speeds, 32
- local, 29-31
- MAC addresses, 49-50
- NAPs (network access points), 34
- OSI (Open Systems Interconnection) model, 48-49
- scanning, 291-298
- system security, 277, 285, 289-291
 - firewalls, 281-282
 - hardening systems, 286
 - IDS, 281-282
 - individual workstation, 285-287
 - patches, 277-278
 - physical, 284-285
 - policies, 282-284
 - ports, 278-281
 - probing, 284
 - professional help, 298-301
 - servers, 287-289
- technologically secured, 250
- VPNs (virtual private networks), 242-244
- new employees, system administration policies, 258**
- New Hacker's Dictionary, 16**
- newsgroups, Usenet, 346-347**
- NICs (network interface cards), 29**
- Nigerian advance-fee scam, 59**
- NIST 800-115 security assessments, 151**
- Nmap port scanner, 139-142**
- NNTP (Network News Transfer Protocol), 33**
- nodes, 41**
- nondisclosure and noncompete agreements, 162**
- nonvirus viruses, 114-115**
- Norton antivirus, 6**

- Norton antivirus software, 127-128, 224**
- Norton Personal Firewall, 281**
- Norton virus scanner, 116**
- notification, IDS, 231**
- NSA (National Security Agency), 285**
 - information assessment methodology, 151-152
- NSA ANT Catalog, 315**
- nslookup command, 47**

O

- Offensive Security, 300**
 - penetration testing certifications, 136
- OMB Circular A-130, 20**
- on-demand virus scanners, 222**
- ongoing virus scanners, 222**
- The Onion Router (TOR), 330-331**
- online security resources, 21**
- Openfiles command, 369**
- operating system utilities, computer forensics, 369-370**
- Operation Ababil, 325**
- operators, IDS, 230**
- OphCrack password cracker, 147-148**
- OR operation, 192**
- Oracle Virtual Box, 383**
- OSForensics tool, 364**
- OSI (Open Systems Interconnection) model, 48-49**
- Outlook viruses, 109**
- Outpost Firewall, 227, 281**
- Oxley, Michael, 269**
- Oxygen tool, 364**

P

packets, 40-41

- filtering and Inspection, firewalls, 225
- headers, 40
- ICMP, 94
 - blocking, 99

Pakistan Cyber Army, 312

PAP (Password Authentication Protocol), 236

pass the hash attacks, 149

passive IDS, 229

passive scanning techniques, hacking, 137-138

Password Authentication Protocol (PAP), 236

password cracking, 146-148

passwords

- age, 283
- history, 283
- policies, 252-253
- quality, 283, 290

patches, checking for, 277-278

payload, steganography, 210

Payment Card Industry Data Security Standards (PCI DSS), 269

Payment Card Industry (PCI) penetration testing standard, 152-153

PCI (Payment Card Industry) penetration testing standard, 152-153

PCI DSS (Payment Card Industry Data Security Standards), 269

PEAP (Protected Extensible Authentication Protocol), 237

penetration testers, 16

penetration testing, 136

- NIST 800-115, 151
- NSA information assessment methodology, 151-152

PCI standard, 152-153

Professional Penetration Tester, 300

perimeter security approach, 18

PGP (Pretty Good Privacy)

- certificates, 239
- encryption, 205-206

phishing, 65

- spear, 175-176

phone taps, industrial espionage, 172

phreaking, 16-17, 137

physical connections, local networks, 29-31

ping command, 39, 45, 87-88

ping of death (PoD), 96

ping scans (Nmap), 140

plain text, 193

planning phase (NIST 800-115 security assessment), 151

plug-ins, Nessus, 296

PoD (ping of death), 96

Point-to-Point Tunneling Protocol (PPTP), 242-243

Poitier, Sidney, 16

policies, security, 250-251, 282-284

- access control, 263-264
- checklists, 283
- data classification, 265
- developmental, 264
- disaster recovery, 266-268
- guidelines, 264
- legal issues, 268-269
- Nessus, 296
- passwords, 283
- procedures, 264
- severity, 283
- standards, 264

- system administration, 258
 - change requests, 259-261
 - departing employees, 258-259
 - DoS attacks, 262
 - hacker intrusion, 262-263
 - new employees, 258
 - security breaches, 261
 - virus infection, 261-262
 - user, 251, 258
 - BYOD (bring your own device), 256-257
 - desktop configuration, 256
 - email usage, 254-255
 - installing/uninstalling software, 255
 - instant messaging, 255-256
 - Internet usage, 253-254
 - passwords, 252-253
 - termination/expulsion, 257
 - polymorphic viruses, 111**
 - POP3 (Post Office Protocol version 3), 33, 39**
 - ports, 31**
 - checking for, 278-281
 - routers, 278
 - scanning, 139-142
 - PPTP (Point-to-Point Tunneling Protocol), 242-243**
 - Preneel, Bart, 208**
 - Pretty Good Privacy (PGP) encryption, 205-206**
 - prime numbers, 202**
 - principal, Kerberos, 238**
 - private information, data classification, 265**
 - private IP addresses, 36**
 - privileges, least, 18, 172**
 - procedures, security policies, 264**
 - professional help, system security, 298-301**
 - Professional Penetration Tester certification, 136**
 - Professional Penetration testers, 300**
 - propaganda, 319**
 - prospective employees, background checks, 338**
 - civil court records, 344
 - general searches, 339-342
 - respecting privacy, 342
 - sex offender registries, 342-344
 - state court records, 345
 - Usenet, 346-347
 - Protected Extensible Authentication Protocol (PEAP), 237**
 - protocols, 33, 41. See also specific protocols**
 - proxy servers, 17, 48**
 - public information, data classification, 265**
 - public IP addresses, 37**
 - public key encryption, 201**
 - Diffie-Hellman, 204-205
 - digital signatures, 207
 - Elliptic Curve, 205
 - fraudulent methods, 206-207
 - PGP (Pretty Good Privacy), 205-206
 - RSA, 202-204
 - X.509 certificates, 239
 - pump and dump, online stock bulletins, 60**
-
- ## Q-R
- Quick Stego, 171**
 - QuickStego, 211**
 - RA (registration authority), 240**
 - Radio Free Europe, 320**
 - RAID levels, 268**

rail fence cipher, 190-191

rainbow tables, 209-210

Rand Corporation cyber terrorism report, 328

ransomware, 111

RC4 block cypher, 199

reconnaissance phase, hacking, 137

active scanning, 139

enumeration, 142-144

port scanning, 139-142

vulnerability assessment, 142

passive scanning, 137-138

recovering deleted files, 366-369

recruiting, cyber terrorism, 330

Redford, Robert, 16

Registry (Windows), 371-374

Rejewsky, Marrian, 191

related-key attacks, 213

relational databases, SQL script injection, 144-146

repeaters, networks, 31

reporting phase (NIST 800-115 security assessment), 151

reports (MBSA), 293

resources, online, 21

retrieving deleted files, 366-369

Richardson, Edward, 68

Rijmen, Vincent, 197

Rijndael block cipher, 197-200

RipeMD, 208

Rivest, Ron, 199, 202, 208-209

RJ-11 jacks, 29

RJ-45 jacks, 29-31

Rombertik virus, 111

rootkits, 124

router-based firewalls, 227

routers

hardening, 286

logging, 291

networks, 31

ports on, 278

TOR (The Onion Router), 330-331

Rozycki, Jerzy, 191

RSA encryption, 202-204

RST cookies, TCP SYN flood attack, 93

Rubin, Andy, 378

Rutkowski, Benjamin, 68

S

SAs (Security Associations), IPsec, 243

sandbox approach, virus scanners, 223

SANS Institute, 285

penetration testing certifications, 136

website, 21

Sarbanes-Oxley Act, 269

Sasser virus/buffer overflow, 120-121

s-boxes, 196

SCADA (Supervisory Control and Data Acquisitions), 318

scams. See fraud

scanning networks, 291-298

scareware, 112

Scherbius, Arthur, 191

Scientific Working Group on Digital Evidence (SWGDE), 362-363

screened host firewalls, 227

script kiddies, 16, 137

Sears, Nick, 378

Secure Sockets Layer (SSL), 240-242

security alerts, 116

Security Associations (SAs), IPsec, 243

security breaches, 6-8

Security log (Windows), 365

security policies, 250-251

access control, 263-264

checklists, 283

data classification, 265

developmental, 264

disaster recovery, 266-268

guidelines, 264

legal issues, 268-269

password quality, 283

procedures, 264

severity, 283

standards, 264

system, 282-284

system administration, 258

change requests, 259-261

departing employees, 258-259

DoS attacks, 262

hacker intrusion, 262-263

new employees, 258

security breaches, 261

virus infection, 261-262

user, 251-252, 257-258

BYOD (bring your own device), 256-257

desktop configuration, 256

email usage, 254-255

installing/uninstalling software, 255

instant messaging, 255-256

Internet usage, 253-254

passwords, 252-253

termination/expulsion, 257

Security+ certifications, 5

sensors, IDS, 230

serial number, X.509 certificates, 239

Serpent block cypher, 199

server rooms, securing, 284

servers

errors, 39

hardening, 286

Nessus, starting, 293-295

proxy, 17, 48

securing, 287-289

services, Windows, shutting down, 279-281

session hijacking, 6, 11

sex offender registries, 342-344

SHA (Secure Hash Algorithm), 208

Shamir, Adi, 202

Shannon, Claude, 206

ShiftRows step (AES), 198

shill bidding, auctions, 62-63

Shiva Password Authentication Protocol (SPAP), 236

signature algorithm identifier, X.509 certificates, 239

Silk Road, 332

SillyFDC worm, 312

SIM (subscriber identity module), 375

Simple Mail Transfer Protocol (SMTP), 33

single-key encryption, 194

AES (Advanced Encryption Standard), 197-200

DES (Data Encryption Standard), 194-196

triple DES, 197

Sinn Fein, 319

Skipjack block cypher, 200

Sleuth Kit tool, 364

SMTP (Simple Mail Transfer Protocol), 33, 39

Smurf IP attacks, 94-95

Sneakers, 16

Snort, 231-235

Snow tool, 211

Snowden, Edward, 12

Sobig virus, 113-114

social engineering, 8, 170

software. See also malware

antispware, 228-229

firewalls, 224-227

IDS (intrusion detection system), 229-235

Norton AntiVirus, 127-128

security policies, 255

virus scanners, 221-224

spam, 126

SPAP (Shiva Password Authentication Protocol), 236

sparse infector viruses, 110

spear phishing, 175-176

specificity, cyber stalking, 69

Specter, 235

spread of viruses, 109-110

spying, industrial. See industrial espionage

spyware, 7, 121

antispware, 228-229

detection and elimination, 127-129

FinFisher, 314-315

Flame, 115, 314

industrial espionage, 171

legal uses, 121

obtaining, 122-123

target delivery, 122

Troj/Invo-Zip, 112

TSPY_FAREIT.YOI, 112

SQL (Structured Query Logic)

commands, 9

script injection, 9-10, 144-146

SSL (Secure Sockets Layer), 240-242

Stacheldraht tool, 91

stack tweaking, TCP SYN flood attack, 93-94

stalking, cyber, 65-70

standards, security policies, 264

Stanford University cryptography history website, 187

state court record searches, 345

stateful packet inspection, firewalls, 225

Stealth Files 4, 211

steganography, 210

industrial espionage, 171

tools, 211

StegVideo, 211

stocks, pump and dump, 60

StopGeorgia.ru forum, 314

stream ciphers, 194

Stuxnet virus, 313-314

SubBytes step (AES), 198

subnetting, 37

subscriber identity module (SIM), 375

substitution alphabet, 188

Supervisory Control and Data Acquisitions (SCADA), 318

SWGDE (Scientific Working Group on Digital Evidence), 362-363

switches, networks, 31

Symantec

cryptography, 185

viruses, 6

symmetric encryption, 194

AES (Advanced Encryption Standard), 197-198

Blowfish, 199

cipher-block chaining, 200

electronic codebook, 200

math, 199

RC4, 199

- Serpent, 199
- Skipjack, 200
- DES (Data Encryption Standard), 194-196
- fraudulent methods, 206-207
- triple DES, 197
- SYN (SYNchronize) bits, 41**
- SYN cookies, TCP SYN flood attack, 92-93**
- SYN scans (Nmap), 140**
- system administration policies, 258**
 - change requests, 259-261
 - departing employees, 258-259
 - DoS attacks, 262
 - hacker intrusion, 262-263
 - new employees, 258
 - security breaches, 261
 - virus infection, 261-262
- System log (Windows), 365**
- system logs, finding evidence in, 365-366**
- system security, 277, 285**
 - firewalls, 281-282
 - hardening systems, 286
 - IDS, 281-282
 - individual workstation, 285-287
 - networks, 289-291
 - scanning, 291-298
 - patches, 277-278
 - physical, 284-285
 - policies, 282-284
 - ports, 278-281
 - probing, 284
 - professional help, 298-301
 - servers, 287-289

T

- TCP SYN flood attack, 91-94**
- TCP/IP protocols, 33-34**
- teardrop attacks, 96**
- technologically secured networks, 250**
- Telnet, 33**
- TeraBIT virus maker, 148-149**
- Terminate and Stay Resident (TSR) program, 221**
- terminators, 29**
- terrorism. See cyber terrorism**
- testing, penetration, 136, 151-153**
- TFN (Tribal Flood Network), 90-91**
- TFTP (Trivial File Transfer Protocol), 33**
- The Onion Router (TOR), 330-331**
- threats. See attacks**
- ticket-granting server (TGS), Kerberos, 238**
- TLS (Transport Layer Security), 240-242**
 - EAP (Extensible Authentication Protocol), 237
- Tomlinson, Ray, 41**
- TOR (The Onion Router), 330-331**
- total breaks, cryptography, 212**
- traceroute command, 39**
- tracert command, 45-46**
- Transport Layer Security (TLS). See TLS (Transport Layer Security)**
- triple DES, 197**
- Trithmeus, Johannes, 171, 211**
- Trivial File Transfer Protocol (TFTP), 33**
- Trojan horses, 7, 116-118**
 - Back Orifice, 117
 - eLiTeWrap, 118
 - EliteWrapper, 117
 - MyDoom, 116
 - Troj/Invo-Zip, 112
- TrueCrypt, 173**
- TSG (ticket-granting server), Kerberos, 238**

TSPY_FAREIT.YOI spyware, 112

TSR (Terminate and Stay Resident) program, 221

Turing, Alan, 192

U

UDP flood attacks, 96

Ugray, Zolt, 14

Ulbricht, Ross, 332

UMTS (Universal Mobile Telecommunications Systems), 376

uniform resource locators (URLs), 39-40

uninstalling software, security policies, 255

unique name of issuer, X.509 certificates, 239

Universal Mobile Telecommunications Systems (UMTS), 376

UNIX operating system, 42

unshielded twisted-pair (UTP) cable, 30

URLs (uniform resource locators), 39-40

USB devices, listing, 373

Usenet, 346-347

user security policies, 251

- BYOD (bring your own device), 256-257
- desktop configuration, 256
- email usage, 254-255
- installing/uninstalling software, 255
- instant messaging, 255-256
- Internet usage, 253-254
- passwords, 252-253
- termination/expulsion, 257

U.S. Secret Service guidelines, computer forensics, 361-362

UTP (unshielded twisted-pair) cable, 30

V

validity period, X.509 certificates, 239

VIA Technology, industrial espionage, 166

Vigenere cipher, 190

Virtual Box (Oracle), 383

Virtual PC, 383

virtual private networks (VPNs). See VPNs (virtual private networks)

virtual servers, 384

virtualization, forensics, 382-384

virulence, 113

virus scanners, 116, 127, 221-224, 250

viruses, 6, 98, 109-111

- armored, 110
- avoiding, 115-116
- Bagle, 114
- BlackEnergy, 315
- CryptoLocker, 111
- CryptoWall, 112
- detection and elimination, 127-129
- FakeAV, 112
- Flame, 115-314
- Gameover Zeus, 111
- MacDefender, 112
- macro, 110
- memory-resident, 110
- Mimail, 114
- Morris worm, 115
- multi-partite, 110
- MyDoom, 116, 311
- nonvirus, 114-115
- polymorphic, 111
- propagation, 109-110
- Rombertik, 111

Sasser, 120-121
 Sobig, 113-114
 sparse infector, 110
 Stuxnet, 313-314
 system administration policies, 261-262
 Troj/Invo-Zip, 112
 versus worms, 117
 virus scanners, 116
 W32/Netsky-P, 112

VMware Workstation, 383

VPNs (virtual private networks), 242

IPsec, 243-244
 L2TP (Layer 2 Tunneling Protocol), 243
 PPTP (Point-to-Point Tunneling Protocol),
 242-243

vulnerability assessments, 142

W

W32/Netsky-P virus, 112

war-driving, 8

weapons, cyber warfare, 313

BlackEnergy, 315
 FinFisher, 314
 Flame, 314
 NSA ANT Catalog, 315
 StopGeorgia.ru, 314
 Stuxnet, 313-314

web attacks, 6, 9-11

web-based mobile code, 125

WEP (Wired Equivalent Privacy), 244

white hat hackers, 15, 137

white hat hacking, 136

WhoIS command, 33

Wi-Fi Protected Access (WPA), 244

Wi-Fi Protected Access2 (WPA2), 244

Wi-Fi security, 244

Wi-Fi sniffing, 8

Williamson, Malcolm J., 205

Windows

computer forensics, 378
 finding evidence in logs, 365
 shutting down services, 279-281

Windows Registry, 371-374

Windows Security templates, 285

Wired Equivalent Privacy (WEP), 244

wireless communication, 29

workstations, securing, 284-287

World Wide Web, 42

worms, 98. See also viruses

Agent.btz, 311
 Morris, 115
 SillyFDC, 312
 Troj/Invo-Zip, 112
 versus viruses, 117
 W32/Netsky-P, 112

WPA (Wi-Fi Protected Access), 244

WPA2 (Wi-Fi Protected Access2), 244

X-Y

X.509 digital certificates, 239-240

XOIC tool, 89-90

XOR operation, 192-193

Yahoo!

news boards, information control, 321
 People Search, 340

Z

Zezev, Oleg, 167

Zhang, Hao, 165

Zimmerman, Phil, 205

Zone Labs firewalls, 227

zone transfers, DNS, 50

ZoneAlarm Security Suite, 227

Zygalski, Henryk, 191