



INFORMATION SECURITY

PRINCIPLES AND PRACTICES

SECOND EDITION

MARK S. MERKOW • JIM BREITHAUP

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

Information Security: Principles and Practices

Second Edition

Mark S. Merkow
Jim Breithaupt

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Information Security: Principles and Practices, Second Edition

Copyright © 2014 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: 978-0-7897-5325-0

ISBN-10: 0-7897-5325-1

Library of Congress Control Number: 2014937271

Printed in the United States of America

First Printing: June 2014

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 authors 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 international@pearsoned.com.

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Jeff Riley

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Krista Hansing Editorial Services, Inc.

Indexer
Publishing Works

Proofreader
Paula Lowell

Technical Editors
Tatyana Zidarov
Chris Crayton

Publishing Coordinator
Vanessa Evans

Cover Designer
Alan Clements

Compositor
Trina Wurst

Contents at a Glance

Preface	xiii
1 Why Study Information Security?.....	2
2 Information Security Principles of Success.....	18
3 Certification Programs and the Common Body of Knowledge.....	36
4 Governance and Risk Management.....	54
5 Security Architecture and Design.....	80
6 Business Continuity Planning and Disaster Recovery Planning	110
7 Law, Investigations, and Ethics.....	126
8 Physical Security Control	146
9 Operations Security.....	166
10 Access Control Systems and Methodology.....	182
11 Cryptography	200
12 Telecommunications, Network, and Internet Security	224
13 Software Development Security.....	260
14 Securing the Future.....	280
A Common Body of Knowledge.....	292
B Security Policy and Standards Taxonomy.....	302
C Sample Policies	306
D HIPAA Security Rule Standards.....	320
Index.....	324

Table of Contents

Preface	xiii
Chapter 1: Why Study Information Security?	2
Introduction	2
The Growing Importance of IT Security and New Career Opportunities	3
An Increase in Demand by Government and Private Industry	4
Becoming an Information Security Specialist	4
Schools Are Responding to Demands	6
The Importance of a Multidisciplinary Approach	7
Contextualizing Information Security	7
Information Security Careers Meet the Needs of Business	8
Summary	11
Test Your Skills	11
Chapter 2: Information Security Principles of Success	18
Introduction	18
Principle 1: There Is No Such Thing As Absolute Security	19
Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability	20
Integrity Models	21
Availability Models	21
Principle 3: Defense in Depth as Strategy	22
Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions	24
Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance	24
Principle 6: Security Through Obscurity Is Not an Answer	25
Principle 7: Security = Risk Management	25
Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive	27
Principle 9: Complexity Is the Enemy of Security	29
Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security	29
Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility	29

Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!	30
Summary	31
Test Your Skills	31
Chapter 3: Certification Programs and the Common Body of Knowledge	36
Introduction	36
Certification and Information Security	37
International Information Systems Security Certifications Consortium (ISC) ² . .	38
The Information Security Common Body of Knowledge	39
Information Security Governance and Risk Management	39
Security Architecture and Design	40
Business Continuity and Disaster Recovery Planning	40
Legal Regulations, Investigations, and Compliance	41
Physical (Environmental) Security	41
Operations Security	42
Access Control	42
Cryptography	42
Telecommunications and Network Security	43
Software Development Security	43
Other Certificate Programs in the IT Security Industry	44
Certified Information Systems Auditor	44
Certified Information Security Manager	44
Certified in Risk and Information Systems Control	44
Global Information Assurance Certifications	44
(ISC) ² Specialization Certificates	45
CCFP: Certified Cyber Forensics Professional	45
HCISPP: HealthCare Information Security and Privacy Practitioner . . .	45
Vendor-Specific and Other Certification Programs	46
Summary	47
Test Your Skills	47
Chapter 4: Governance and Risk Management	54
Introduction	54
Security Policies Set the Stage for Success	55
Understanding the Four Types of Policies	57

Programme-Level Policies	57
Programme-Framework Policies	59
Issue-Specific Policies	60
System-Specific Policies	61
Developing and Managing Security Policies	62
Security Objectives	62
Operational Security	62
Policy Implementation.	63
Providing Policy Support Documents.	64
Regulations	64
Standards and Baselines	66
Guidelines	67
Procedures.	67
Suggested Standards Taxonomy	67
Asset and Data Classification.	67
Separation of Duties	68
Employment Hiring Practices.	69
Risk Analysis and Management.	70
Education, Training, and Awareness	72
Who Is Responsible for Security?	73
Summary.	74
Test Your Skills.	74
Chapter 5: Security Architecture and Design	80
Introduction.	80
Defining the Trusted Computing Base	81
Rings of Trust.	81
Protection Mechanisms in a TCB	84
System Security Assurance Concepts.	86
Goals of Security Testing	86
Formal Security Testing Models.	87
The Trusted Computer Security Evaluation Criteria	87
Division D: Minimal Protection	88
Division C: Discretionary Protection	88

Division B: Mandatory Protection	88
Division A: Verified Protection	90
The Trusted Network Interpretation of the TCSEC	91
The Information Technology Security Evaluation Criteria	91
Comparing ITSEC to TCSEC	91
ITSEC Assurance Classes	92
The Canadian Trusted Computer Product Evaluation Criteria	93
The Federal Criteria for Information Technology Security	93
The Common Criteria	94
Protection Profile Organization.	95
Security Functional Requirements	96
Evaluation Assurance Levels	98
The Common Evaluation Methodology	100
Confidentiality and Integrity Models	101
Bell-LaPadula Model.	101
Biba Integrity Model	102
Advanced Models	102
Summary	104
Test Your Skills	104
Chapter 6: Business Continuity Planning and Disaster Recovery Planning	110
Introduction.	110
Overview of the Business Continuity Plan and Disaster Recovery Plan	111
Why the BCP Is So Important	112
Types of Disruptive Events	113
Defining the Scope of the BCP	114
Creating the Business Impact Analysis	114
Disaster Recovery Planning.	115
Identifying Recovery Strategies	116
Understanding Shared-Site Agreements.	116
Using Alternate Sites	116
Making Additional Arrangements.	117
Testing the DRP	118

Summary	120
Test Your Skills	120
Chapter 7: Law, Investigations, and Ethics	126
Introduction	126
Types of Computer Crime	127
How Cybercriminals Commit Crimes	128
The Computer and the Law	129
Legislative Branch of the Legal System	130
Administrative Branch of the Legal System	130
Judicial Branch of the Legal System	130
Intellectual Property Law	131
Patent Law	131
Trademarks	132
Trade Secrets	132
Privacy and the Law	133
International Privacy Issues	133
Privacy Laws in the United States	134
Computer Forensics	135
The Information Security Professional's Code of Ethics	136
Other Ethics Standards	137
Computer Ethics Institute	138
Internet Activities Board: Ethics and the Internet	138
Code of Fair Information Practices	139
Summary	140
Test Your Skills	140
Chapter 8: Physical Security Control	146
Introduction	146
Understanding the Physical Security Domain	147
Physical Security Threats	148
Providing Physical Security	149
Summary	160
Test Your Skills	160

Chapter 9: Operations Security	166
Introduction	166
Operations Security Principles	167
Operations Security Process Controls	168
Operations Security Controls in Action	170
Software Support	171
Configuration and Change Management	171
Backups	172
Media Controls	172
Documentation	174
Maintenance	174
Interdependencies	175
Summary	177
Test Your Skills	177
Chapter 10: Access Control Systems and Methodology	182
Introduction	182
Terms and Concepts	183
Identification	183
Authentication	183
Least Privilege (Need to Know)	183
Information Owner	184
Discretionary Access Control	184
Access Control Lists	184
User Provisioning	194
Mandatory Access Control	185
Role-Based Access Control	185
Principles of Authentication	186
The Problems with Passwords	186
Multifactor Authentication	188
Biometrics	189
Single Sign-On	190
Kerberos	191
Federated Identities	192

Remote User Access and Authentication.	192
Remote Access Dial-In User Service.	193
Virtual Private Networks	193
Summary.	194
Test Your Skills.	194
Chapter 11: Cryptography	200
Introduction.	200
Applying Cryptography to Information Systems	201
Basic Terms and Concepts	201
Strength of Cryptosystems	203
Cryptosystems Answer the Needs of Today's E-Commerce.	205
The Role of Keys in Cryptosystems.	206
Putting the Pieces to Work	209
Digesting Data	209
Digital Certificates	212
Examining Digital Cryptography	214
Hashing Functions.	214
Block Ciphers	214
Implementations of PPK Cryptography.	215
Summary.	218
Test Your Skills.	218
Chapter 12: Telecommunications, Network, and Internet Security	224
Introduction.	224
An Overview of Network and Telecommunications Security	225
Network Security in Context	226
The Open Systems Interconnection Reference Model	226
The Protocol Stack	226
The OSI Reference Model and TCP/IP	229
The OSI Model and Security	231
Data Network Types.	233
Local Area Networks.	233
Wide Area Networks	233
Internet	233

Intranet	234
Extranet	234
Protecting TCP/IP Networks	234
Basic Security Infrastructures	235
Routers	236
Firewalls	237
Intrusion Detection Systems	245
Intrusion Prevention Systems	248
Virtual Private Networks	249
IPSec	249
Encapsulating Security Protocol	251
Security Association	251
Internet Security Association and Key Management Protocol	252
Security Policies	252
IPSec Key Management	253
Applied VPNs	253
Cloud Computing	254
Summary	255
Test Your Skills	255
Chapter 13: Software Development Security	260
Introduction	260
The Practice of Software Engineering	261
Software Development Life Cycles	261
Don't Bolt Security On—Build It In	263
Catch Problems Sooner Rather Than Later	264
Requirements Gathering and Analysis	265
Systems Design and Detailed Design	266
Design Reviews	267
Development (Coding) Phase	268
Testing	270
Deployment	270
Security Training	272

Measuring the Secure Development Program	272
Open Software Assurance Maturity Model (OpenSAMM)	272
Building Security in Maturity Model (BSIMM)	272
Summary	273
Test Your Skills	273
Chapter 14: Securing the Future	280
Introduction	280
Operation Eligible Receiver	281
Carders, Account Takeover, and Identity Theft	282
Some Definitions	282
Zeus Banking Trojan	282
Phishing and Spear Phishing	283
Other Trends in Internet (In)Security	284
The Year (Decade?) of the Breach	284
The Rosy Future for InfoSec Specialists	285
Summary	286
Test Your Skills	286
Appendix A: Common Body of Knowledge	292
Access Control	292
Telecommunications and Network Security	293
Information Security Governance and Risk Management	294
Software Development Security	295
Cryptography	296
Security Architecture and Design	297
Operations Security	298
Business Continuity and Disaster Recovery Planning	299
Legal Regulations, Investigations, and Compliance	300
Physical (Environmental) Security	301
Appendix B: Security Policy and Standards Taxonomy	302
Appendix C: Sample Policies	306
Sample Computer Acceptable Use Policy	306
1.0.0 Acceptable Use Policy	306

Sample Email Use Policy	310
1.0.0 Email Use Policy	310
Sample Password Policy	312
1.0.0 Password Policy	312
Sample Wireless (WiFi) Use Policy	317
1.0.0 Wireless Communication Policy	317
Appendix D: HIPAA Security Rule Standards	320
HIPAA Security Standards	320
Administrative Procedures	321
Physical Safeguards	321
Technical Security Services	322
Technical Security Mechanisms	322
Index	324

Preface

When teaching a complex and ever-changing discipline such as information security, students are best served by beginning with a high-level understanding of the subject before they tackle the details. A solid grasp of the objectives, terminology, principles, and frameworks will help them understand how to place issues in a proper context for determining working solutions. That is the goal of this text: to introduce students to the most important topics of information security and pique their interest to learn more.

The body of knowledge (as it is called in the IT security industry) is vast, deep, and, at times, baffling. Solutions are not always straightforward because the problems they address are rarely intuitive. No cookbook or universal recipe for IT security success exists. Ideally, protecting computer systems from attacks and unauthorized access means anticipating problems and devising strategies to address how people, processes, and technologies interact. The goal, although not always realistic, is to prevent these problems from happening instead of simply reacting to them as so many organizations do today.

This is rarely easy.

This book navigates the ocean of information technology (IT) security issues while keeping the technical jargon to a minimum. Chapters are ordered to follow the major “domains” of the Common Body of Knowledge, to help prepare students for a more detailed examination of the topics, if that is their desire.

If you decide to enter the field of information security, you’ll find this book helpful in charting your course in joining the ranks of professionals and specialists in information security.

About the Authors

Mark Merkow, CISSP, CISM, CSSLP, is a technical director for a Fortune 100 financial services firm, where he works on implementing and operating a software security practice for the enterprise. He has more than 35 years of IT experience, including 20 years in IT security. Mark has worked in a variety of roles, including applications development, systems analysis and design, security engineering, and security management. Mark holds a master's degree in decision and info systems from Arizona State University (ASU), a master's of education in Distance Learning from ASU, and a bachelor's degree in Computer Info Systems from ASU.

Jim Breithaupt is a data integrity manager for a major bank, where he manages risk for a large data mart. He has more than 30 years of data processing experience and has co-authored several other books on information systems and information security, along with Mark Merkow.

Acknowledgments

From Mark Merkow:

To begin, I'm deeply grateful to my friend and co-author, Jim, who has an amazing ability to turn the obscure into the transparent. Without Jim, there would be no book.

Thanks to my wife, Amy Merkow, as always, for her positive attitude, full support, and unwavering belief in the written word.

I also want to thank our far-scattered children, Josh Merkow, Jasmine Merkow, Brandon Bohlman, and Caitlyn Bohlman, for their support throughout the writing process.

Tremendous thanks goes to Betsy Brown, Tonya Simpson, and the entire staff at Pearson, along with Jeff Riley at Box Twelve Communications, for their commitment to excellence, efficiency, and positive attitude, all of which make working with them a total pleasure.

Special thanks goes to my agent, Carole Jelen at Waterside Productions, for the remarkable effort that goes into book contracting and publication.

From Jim Breithaupt:

First, I would like to thank Mark Merkow for being the guiding light of every writing project he has asked me to share with him. If it weren't for Mark's extensive knowledge of data processing and his enthusiasm for our endeavors, this book, like all the others, would never have come to fruition. I would also like to acknowledge Margaret and my children, Faye and Bo, who are my joy and inspiration. Finally, I'd like to give a tip of the hat to Carole Jelen with Waterside Productions for her assistance, and to the fine technical reviewers and editors at Pearson for helping make this book possible.

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

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

This page intentionally left blank

This page intentionally left blank

Chapter | 2

Information Security Principles of Success

Chapter Objectives

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

- Build an awareness of 12 generally accepted basic principles of information security to help you determine how these basic principles apply to real-life situations
- Distinguish among the three main security goals
- Learn how to design and apply the principle of defense in depth
- Comprehend human vulnerabilities in security systems to better design solutions to counter them
- Explain the difference between functional requirements and assurance requirements
- Comprehend the fallacy of security through obscurity to avoid using it as a measure of security
- Comprehend the importance of risk-analysis and risk-management tools and techniques for balancing the needs of business
- Determine which side of the open disclosure debate you would take

Introduction

Many of the topics information technology students study in school carry directly from the classroom to the workplace. For example, new programming and systems analysis and design skills can often be applied on new systems-development projects as companies espouse cloud computing and mobile infrastructures that access internal systems.

Security is a little different. Although their technical skills are certainly important, the best security specialists combine their practical knowledge of computers and networks with general theories about security, technology, and human nature. These concepts, some borrowed from other fields, such as military defense, often take years of (sometimes painful) professional experience to learn. With a conceptual and principled view of information security, you can analyze a security need in the right frame of reference or context so you can balance the needs of permitting access against the risk of allowing such access. No two systems or situations are identical, and no cookbooks can specify how to solve certain security problems. Instead, you must rely on principle-based analysis and decision making.

This chapter introduces these key information security principles, concepts, and durable “truths.”

Principle 1: There Is No Such Thing As Absolute Security

In 2003, the art collection of the Whitworth Gallery in Manchester, England, included three famous paintings by Van Gogh, Picasso, and Gauguin. Valued at more than \$7 million, the paintings were protected by closed-circuit television (CCTV), a series of alarm systems, and 24-hour rolling patrols. Yet in late April 2003, thieves broke into the museum, evaded the layered security system, and made off with the three masterpieces. Several days later, investigators discovered the paintings in a nearby public restroom along with a note from the thieves saying, “The intention was not to steal, only to highlight the woeful security.”

The burglars’ lesson translates to the information security arena and illustrates the first principle of information security (IS): Given enough time, tools, skills, and inclination, a malicious person can break through any security measure. This principle applies to the physical world as well and is best illustrated with an analogy of safes or vaults that businesses commonly use to protect their assets. Safes are rated according to their resistance to attacks using a scale that describes how long it could take a burglar to open them. They are divided into categories based on the level of protection they can deliver and the testing they undergo. Four common classes of safe ratings are B-Rate, C-Rate, UL TL-15, and UL TL-30:

- **B-Rate:** B-Rate is a catchall rating for any box with a lock on it. This rating describes the thickness of the steel used to make the lockbox. No actual testing is performed to gain this rating.
- **C-Rate:** This is defined as a variably thick steel box with a 1-inch-thick door and a lock. No tests are conducted to provide this rating, either.
- **UL TL-15:** Safes with an Underwriters Laboratory (UL) TL-15 rating have passed standardized tests as defined in UL Standard 687 using tools and an expert group of safe-testing engineers. The UL TL-15 label requires that the safe be constructed of 1-inch solid steel or equivalent. The label means that the safe has been tested for a net working time of 15 minutes using “common hand tools, drills, punches hammers, and pressure applying devices.” *Net working time* means that when the tool comes off the safe, the clock stops. Engineers exercise more than 50 different types of attacks that have proven effective for safecracking.

- **UL TL-30:** UL TL-30 testing is essentially the same as the TL-15 testing, except for the net working time. Testers get 30 minutes and a few more tools to help them gain access. Testing engineers usually have a safe's manufacturing blueprints and can disassemble the safe before the test begins to see how it works.

FYI: Confidentiality by Another Name

Confidentiality is sometimes referred to as the principle of least privilege, meaning that users should be given only enough privilege to perform their duties, and no more. Some other synonyms for confidentiality you might encounter include *privacy*, *secrecy*, and *discretion*.

As you learn in Chapter 5, "Security Architecture and Design," security testing of hardware and software systems employs many of the same concepts of safe testing, using computers and custom-developed testing software instead of tools and torches. The outcomes of this testing are the same, though: As with software, no safe is burglar proof; security measures simply buy time. Of course, buying time is a powerful tool. Resisting attacks long enough provides the opportunity to catch the attacker in the act and to quickly recover from the incident. This leads to the second principle.

FYI: Confidentiality Models

Confidentiality models are primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible. Common confidentiality controls are user IDs and passwords.

Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability

All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs (see Figure 2.1). Information security professionals who create policies and procedures (often referred to as governance models) must consider each goal when creating a plan to protect a computer system.



FIGURE 2.1 The CIA triad.

FYI: CIA Triad

The principle of information security protection of confidentiality, integrity, and availability cannot be overemphasized: This is central to all studies and practices in IS. You'll often see the term *CIA triad* to illustrate the overall goals for IS throughout the research, guidance, and practices you encounter.

Integrity Models

Integrity models keep data pure and trustworthy by protecting system data from intentional or accidental changes. Integrity models have three goals:

- Prevent unauthorized users from making modifications to data or programs
- Prevent authorized users from making improper or unauthorized modifications
- Maintain internal and external consistency of data and programs

An example of integrity checks is balancing a batch of transactions to make sure that all the information is present and accurately accounted for.

Availability Models

Availability models keep data and resources available for authorized use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:

- Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered)
- Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)
- Equipment failures during normal use

Some activities that preserve confidentiality, integrity, and/or availability are granting access only to authorized personnel, applying encryption to information that will be sent over the Internet or stored on digital media, periodically testing computer system security to uncover new vulnerabilities, building software defensively, and developing a disaster recovery plan to ensure that the business can continue to exist in the event of a disaster or loss of access by personnel.

Principle 3: Defense in Depth as Strategy

A bank would never leave its assets inside an unguarded safe alone. Typically, access to the safe requires passing through layers of protection that might include human guards and locked doors with special access controls. Furthermore, the room where the safe resides could be monitored by closed-circuit television, motion sensors, and alarm systems that can quickly detect unusual activity. The sound of an alarm might trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas.

Layered security, as in the previous example, is known as defense in depth. This security is implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response. Defense in depth also seeks to offset the weaknesses of one security layer by the strengths of two or more layers.

In the information security world, defense in depth requires layering security devices in a series that protects, detects, and responds to attacks on systems. For example, a typical Internet-attached network designed with security in mind includes routers, firewalls, and intrusion detection systems (IDS) to protect the network from would-be intruders; employs traffic analyzers and real-time human monitors who watch for anomalies as the network is being used to detect any breach in the layers of protection; and relies on automated mechanisms to turn off access or remove the system from the network in response to the detection of an intruder.

Finally, the security of each of these mechanisms must be thoroughly tested before deployment to ensure that the integrated system is suitable for normal operations. After all, a chain is only as good as its weakest link.

In Practice

Phishing for Dollars

Phishing is another good example of how easily intelligent people can be duped into breaching security. Phishing is a dangerous Internet scam, and is becoming increasingly dangerous as targets are selected using data available from social media and enable a malicious person to build a profile of the target to better convince him the scam is real. A phishing scam typically operates as follows:

- The victim receives an official-looking email message purporting to come from a trusted source, such as an online banking site, PayPal, eBay, or other service where money is exchanged, moved, or managed.
- The email tells the user that his or her account needs updating immediately or will be suspended within a certain number of days.
- The email contains a URL (link) and instructs the user to click on the link to access the account and update the information. The link text appears as though it will take the user to the expected site. However, the link is actually a link to the attacker's site, which is made to look exactly like the site the user expects to see.
- At the spoofed site, the user enters his or her credentials (ID and password) and clicks Submit.
- The site returns an innocuous message, such as "We're sorry—we're unable to process your transaction at this time," and the user is none the wiser.
- At this point, the victim's credentials are stored on the attacker's site or sent via email to the perpetrator, where they can be used to log in to the *real* banking or exchange site and empty the account before the user knows what happened.

Phishing and resultant ID theft and monetary losses are on the increase and will begin to slow only after the cycle is broken through awareness and education. Protect yourself by taking the following steps:

- Look for telltale signs of fraud: Instead of addressing you by name, a phishing email addresses you as "User" or by your email address; a legitimate message from legitimate companies uses your name as they know it.
- Do not click on links embedded in unsolicited finance-related email messages. A link might look legitimate, but when you click on it, you could be redirected to the site of a phisher. If you believe that your account is in jeopardy, type in the known URL of the site in a new browser window and look for messages from the provider after you're logged in.
- Check with your provider for messages related to phishing scams that the company is aware of. Your bank or other financial services provider wants to make sure you don't fall victim and will often take significant measures to educate users on how to prevent problems.

Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

The primary reason identity theft, viruses, worms, and stolen passwords are so common is that people are easily duped into giving up the secrets technologies use to secure systems. Organizers of Infosecurity Europe, Britain's biggest information technology security exhibition, sent researchers to London's Waterloo Station to ask commuters to hand over their office computer passwords in exchange for a free pen. Three-quarters of respondents revealed the information immediately, and an additional 15 percent did so after some gentle probing. Study after study like this one shows how little it takes to convince someone to give up their credentials in exchange for trivial or worthless goods.

Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

Functional requirements describe what a system *should* do. Assurance requirements describe how functional requirements should be implemented and tested. Both sets of requirements are needed to answer the following questions:

- Does the system do the right things (behave as promised)?
- Does the system do the right things in the right way?

These are the same questions that others in noncomputer industries face with verification and validation. Verification is the process of confirming that one or more predetermined requirements or specifications are met. Validation then determines the correctness or quality of the mechanisms used to meet the needs. In other words, you can develop software that addresses a need, but it might contain flaws that could compromise data when placed in the hands of a malicious user.

Consider car safety testing as an example. Verification testing for seat belt functions might include conducting stress tests on the fabric, testing the locking mechanisms, and making certain the belt will fit the intended application, thus completing the functional tests. Validation, or assurance testing, might then include crashing the car with crash-test dummies inside to "prove" that the seat belt is indeed safe when used under normal conditions and that it can survive under harsh conditions.

With software, you need both verification and validation answers to gain confidence in products before launching them into a wild, hostile environment such as the Internet. Most of today's commercial off-the-shelf (COTS) software and systems stop at the first step, verification, without bothering to test for obvious security vulnerabilities in the final product. Developers of software generally lack the wherewithal and motivation needed to try to break their own software. More often, developers test that the software meets the specifications in each function that is present but usually do not try to find ways to circumvent the software and make it fail. You learn more about security testing of software in Chapter 5.

Principle 6: Security Through Obscurity Is Not an Answer

Many people in the information security industry believe that if malicious attackers don't know how software is secured, security is better. Although this might seem logical, it's actually untrue. Security through obscurity means that hiding the details of the security mechanisms is sufficient to secure the system alone. An example of security through obscurity might involve closely guarding the written specifications for security functions and preventing all but the most trusted people from seeing it. Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all.

If the security of a system is maintained by keeping the implementation of the system a secret, the entire system collapses when the first person discovers how the security mechanism works—and someone is always determined to discover these secrets. The better bet is to make sure no one mechanism is responsible for the security of the entire system. Again, this is defense in depth in everything related to protecting data and resources.

In Chapter 11, "Cryptography," you'll see how this principle applies and why it makes no sense to keep an algorithm for cryptography secret when the security of the system should rely on the cryptographic keys used to protect data or authenticate a user. You can also see this in action with the open-source movement: Anyone can gain access to program (source) code, analyze it for security problems, and then share with the community improvements that eliminate vulnerabilities and/or improve the overall security through simplification (see Principle 9).

Principle 7: Security = Risk Management

It's critical to understand that spending more on securing an asset than the intrinsic value of the asset is a waste of resources. For example, buying a \$500 safe to protect \$200 worth of jewelry makes no practical sense. The same is true when protecting electronic assets. All security work is a careful balance between the level of risk and the expected reward of expending a given amount of resources. Security is concerned not with eliminating all threats within a system or facility, but with eliminating known threats and minimizing losses if an attacker succeeds in exploiting a vulnerability. Risk analysis and risk management are central themes to securing information systems. When risks are well understood, three outcomes are possible:

- The risks are mitigated (countered).
- Insurance is acquired against the losses that would occur if a system were compromised.
- The risks are accepted and the consequences are managed.

Risk assessment and risk analysis are concerned with placing an economic value on assets to best determine appropriate countermeasures that protect them from losses.

The simplest form of determining the degree of a risk involves looking at two factors:

- What is the consequence of a loss?
- What is the likelihood that this loss will occur?

Figure 2.2 illustrates a matrix you can use to determine the degree of a risk based on these factors.

Likelihood	Consequences				
	1. Insignificant	2. Minor	3. Moderate	4. Major	6. Catastrophic
A (almost certain)	High	High	Extreme	Extreme	Extreme
B (likely)	Moderate	High	High	Extreme	Extreme
C (moderate)	Low	Moderate	High	Extreme	Extreme
D (unlikely)	Low	Low	Moderate	High	Extreme
E (rare)	Low	Low	Moderate	High	High

FIGURE 2.2 Consequences/likelihood matrix for risk analysis.

After determining a risk rating, one of the following actions could be required:

- **Extreme risk:** Immediate action is required.
- **High risk:** Senior management's attention is needed.
- **Moderate risk:** Management responsibility must be specified.
- **Low risk:** Management is handled by routine procedures.

In the real world, risk management is more complicated than simply making a human judgment call based on intuition or previous experience with a similar situation. Recall that every system has unique security issues and considerations, so it's imperative to understand the specific nature of data the system will maintain, what hardware and software will be used to deploy the system, and the security skills of the development teams. Determining the likelihood of a risk coming to life requires understanding a few more terms and concepts:

- Vulnerability
- Exploit
- Attacker

Vulnerability refers to a known problem within a system or program. A common example in InfoSec is called the buffer overflow or buffer overrun vulnerability. Programmers tend to be trusting and not worry about who will attack their programs, but instead worry about who will use their programs legitimately. One feature of most programs is the capability for a user to “input” information or requests. The program instructions (source code) then contain an “area” in memory (buffer) for these inputs and act upon them when told to do so. Sometimes the programmer doesn’t check to see if the input is proper or innocuous. A malicious user, however, might take advantage of this weakness and overload the input area with more information than it can handle, crashing or disabling the program. This is called buffer overflow, and it can permit a malicious user to gain control over the system. This common vulnerability with software must be addressed when developing systems. Chapter 13, “Software Development Security,” covers this in greater detail.

An exploit is a program or “cookbook” on how to take advantage of a specific vulnerability. It might be a program that a hacker can download over the Internet and then use to search for systems that contain the vulnerability it’s designed to exploit. It might also be a series of documented steps on how to exploit the vulnerability after an attacker finds a system that contains it.

An attacker, then, is the link between a vulnerability and an exploit. The attacker has two characteristics: skill and will. Attackers either are skilled in the art of attacking systems or have access to tools that do the work for them. They have the will to perform attacks on systems they do not own and usually care little about the consequences of their actions.

In applying these concepts to risk analysis, the IS practitioner must anticipate who might want to attack the system, how capable the attacker might be, how available the exploits to a vulnerability are, and which systems have the vulnerability present.

Risk analysis and risk management are specialized areas of study and practice, and the IS professionals who concentrate in these areas must be skilled and current in their techniques. You can find more on risk management in Chapter 4, “Governance and Risk Management.”

Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

Controls (such as documented processes) and countermeasures (such as firewalls) must be implemented as one or more of these previous types, or the controls are not there for the purposes of security. Shown in another triad, the principle of defense in depth dictates that a security mechanism serve a purpose by preventing a compromise, detecting that a compromise or compromise attempt is underway, or responding to a compromise while it’s happening or after it has been discovered.

Referring to the example of the bank vault in Principle 3, access to a bank’s safe or vault requires passing through layers of protection that might include human guards and locked doors with special access controls (prevention). In the room where the safe resides, closed-circuit televisions, motion sensors, and alarm systems quickly detect any unusual activity (detection). The sound of an alarm could trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas (response).

These controls are the basic toolkit for the security practitioner who mixes and matches them to carry out the objectives of confidentiality, integrity, and/or availability by using people, processes, or technology (see Principle 11) to bring them to life.

In Practice

How People, Process, and Technology Work in Harmony

To illustrate how people, process, and technology work together to secure systems, let's take a look at how the security department grants access to users for performing their duties. The process, called user access request, is initiated when a new user is brought into the company or switches department or role within the company. The user access request form is initially completed by the user and approved by the manager.

When the user access request is approved, it's routed to information security access coordinators to process using the documented procedures for granting access. After access is granted and the process for sharing the user's ID and password is followed, the system's technical access control system takes over. It protects the system from unauthorized access by requiring a user ID and password, and it prevents password guessing from an unauthorized person by limiting the number of attempts to three before locking the account from further access attempts.

In Practice

To Disclose or Not to Disclose—That Is the Question!

Having specific knowledge of a security vulnerability gives administrators the knowledge to properly defend their systems from related exploits. The ethical question is, how should that valuable information be disseminated to the good guys while keeping it away from the bad guys? The simple truth is, you can't really do this. Hackers tend to communicate among themselves far better than professional security practitioners ever could. Hackers know about most vulnerabilities long before the general public gets wind of them. By the time the general public is made aware, the hacker community has already developed a workable exploit and disseminated it far and wide to take advantage of the flaw before it can be patched or closed down.

Because of this, open disclosure benefits the general public far more than is acknowledged by the critics who claim that it gives the bad guys the same information.

Here's the bottom line: If you uncover an obvious problem, raise your hand and let someone who can do something about it know. If you see something, say something. You'll sleep better at night!

Principle 9: Complexity Is the Enemy of Security

The more complex a system gets, the harder it is to secure. With too many “moving parts” or interfaces between programs and other systems, the system or interfaces become difficult to secure while still permitting them to operate as intended. You learn in Chapter 5 how complexity can easily get in the way of comprehensive testing of security mechanisms.

Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security

At one time, “scaring” management into spending resources on security to avoid the unthinkable was effective. The tactic of fear, uncertainty, and doubt (FUD) no longer works: Information security and IT management is too mature. Now IS managers must justify all investments in security using techniques of the trade. Although this makes the job of information security practitioners more difficult, it also makes them more valuable because of management’s need to understand what is being protected and why. When spending resources can be justified with good, solid business rationale, security requests are rarely denied.

Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

As described in Principle 3, “Defense in Depth as Strategy,” the information security practitioner needs a series of countermeasures and controls to implement an effective security system. One such control might be dual control, a practice borrowed from the military. The U.S. Department of Defense uses a dual control protocol to secure the nation’s nuclear arsenal. This means that at least two on-site people must agree to launch a nuclear weapon. If one person were in control, he or she could make an error in judgment or act maliciously for whatever reason. But with dual control, one person acts as a countermeasure to the other: Chances are less likely that both people will make an error in judgment or act maliciously. Likewise, no one person in an organization should have the ability to control or close down a security activity. This is commonly referred to as separation of duties.

Process controls are implemented to ensure that different people can perform the same operations exactly in the same way each time. Processes are documented as procedures on how to carry out an activity related to security. The process of configuring a server operating system for secure operations is documented as one or more procedures that security administrators use and can be verified as done correctly.

Just as the information security professional might establish process controls to make sure that a single person cannot gain complete control over a system, you should never place all your faith in technology. Technology can fail, and without people to notice and fix technical problems, computer

systems would stall permanently. An example of this type of waste is installing an expensive firewall system (a network perimeter security device that blocks traffic) and then turning around and opening all the ports that are intended to block certain traffic from entering the network.

People, process, and technology controls are essential elements of several areas of practice in information technology (IT) security, including operations security, applications development security, physical security, and cryptography. These three pillars of security are often depicted as a three-legged stool (see Figure 2.3).

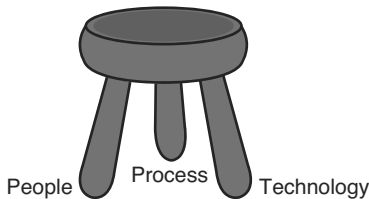


FIGURE 2.3 The people, process, and technology triad.

Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

A raging and often heated debate within the security community and software developing centers concerns whether to let users know about a problem before a fix or patch can be developed and distributed. Principle 6 tells us that security through obscurity is not an answer: Keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security. Users have a right to know about defects in the products they purchase, just as they have a right to know about automobile recalls because of defects. The need to know trumps the need to keep secrets, to give users the right to protect themselves.

Summary

To be most effective, computer security specialists not only must know the technical side of their jobs, but also must understand the principles behind information security. No two situations that security professionals review are identical, and there are no recipes or cookbooks on universal security measures. Because each situation calls for a distinct judgment to address the specific risks inherent in information systems, principles-based decision making is imperative. An old saying goes, “If you only have a hammer, every problem looks like a nail.” This approach simply does not serve today’s businesses, which are always striving to balance risk and reward of access to electronic records. The goal is to help you create a toolkit and develop the skills to use these tools like a master craftsman. Learn these principles and take them to heart, and you’ll start out much further along than your peers who won’t take the time to bother learning them!

As you explore the rest of the Common Body of Knowledge (CBK) domains, try to relate the practices you find to one or more of these. For example, Chapter 8, “Physical Security Control,” covers physical security, which addresses how to limit access to physical spaces and hardware to authorized personnel. This helps prevent breaches in confidentiality, integrity, and availability, and implements the principle of defense in depth. As you will find, these principles are mixed and matched to describe why certain security functions and operations exist in the real world of IT.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following represents the three goals of information security?
 - A. Confidentiality, integrity, and availability
 - B. Prevention, detection, and response
 - C. People controls, process controls, and technology controls
 - D. Network security, PC security, and mainframe security
2. Which of the following terms best describes the assurance that data has not been changed unintentionally due to an accident or malice?
 - A. Availability
 - B. Confidentiality
 - C. Integrity
 - D. Auditability

3. Related to information security, confidentiality is the opposite of which of the following?
 - A. Closure
 - B. Disclosure
 - C. Disaster
 - D. Disposal
4. The CIA triad is often represented by which of the following?
 - A. Triangle
 - B. Diagonal
 - C. Ellipse
 - D. Circle
5. Defense in depth is needed to ensure that which three mandatory activities are present in a security system?
 - A. Prevention, response, and prosecution
 - B. Response, collection of evidence, and prosecution
 - C. Prevention, detection, and response
 - D. Prevention, response, and management
6. Which of the following statements is true?
 - A. The weakest link in any security system is the technology element.
 - B. The weakest link in any security system is the process element.
 - C. The weakest link in any security system is the human element.
 - D. Both B and C
7. Which of the following best represents the two types of IT security requirements?
 - A. Functional and logical
 - B. Logical and physical
 - C. Functional and assurance
 - D. Functional and physical
8. Security functional requirements describe which of the following?
 - A. What a security system should do by design
 - B. What controls a security system must implement
 - C. Quality assurance description and testing approach
 - D. How to implement the system

9. Which of the following statements is true?
- A. Security assurance requirements describe how to test the system.
 - B. Security assurance requirements describe how to program the system.
 - C. Security assurance requirements describe to what degree the testing of the system is conducted.
 - D. Security assurance requirements describe implementation considerations.
10. Which of the following terms best describes the probability that a threat to an information system will materialize?
- A. Threat
 - B. Vulnerability
 - C. Hole
 - D. Risk
11. Which of the following terms best describes the absence or weakness in a system that may possibly be exploited?
- A. Vulnerability
 - B. Threat
 - C. Risk
 - D. Exposure
12. Which of the following statements is true?
- A. Controls are implemented to eliminate risk and eliminate the potential for loss.
 - B. Controls are implemented to mitigate risk and reduce the potential for loss.
 - C. Controls are implemented to eliminate risk and reduce the potential for loss.
 - D. Controls are implemented to mitigate risk and eliminate the potential for loss.
13. Which of the following terms best describes a cookbook on how to take advantage of a vulnerability?
- A. Risk
 - B. Exploit
 - C. Threat
 - D. Program

14. Which of the following represents the three types of security controls?
- A. People, functions, and technology
 - B. People, process, and technology
 - C. Technology, roles, and separation of duties
 - D. Separation of duties, processes, and people
15. Which of the following statements is true?
- A. Process controls for IT security include assignment of roles for least privilege.
 - B. Process controls for IT security include separation of duties.
 - C. Process controls for IT security include documented procedures.
 - D. All of the above

EXERCISES

EXERCISE 2.1: Understanding the Importance of Information Confidentiality

Why is confidentiality important to corporate information? What kinds of abuses can you think of in the absence of controls on confidentiality? What criminal activities could be reduced or eliminated if confidentiality controls were effectively implemented?

EXERCISE 2.2: Evaluating Real-World Defense in Depth

Find some analogies to the principle of defense in depth in the physical world, and make some diagrams of the mechanism you locate. Consider how a bank implements defense in depth and how corporations protect themselves from intruders entering their buildings.

EXERCISE 2.3: Avoiding Security Through Obscurity

Why is security through obscurity a bad idea for the overall security of a system?

EXERCISE 2.4: Identifying a Phishing Scam

Go to www.opendns.com/phishing-quiz/ and take the “Think You Can Outsmart Internet Scammers?” quiz. How well did you perform at identifying phishing scams?

EXERCISE 2.5: Evaluating Risk Management

Every day, you make risk-management decisions in your daily life. Should you get in the car and drive to the store? Should you jaywalk or cross at the light? Should you get on that airplane? Think about the risk-management decisions you make when using your PC:

1. What kinds of judgments do you make before downloading a piece of software?
2. What kinds of judgments do you make before writing an email to your boss?
3. What mental steps do you go through before taking some action?

PROJECTS

PROJECT 2.1: Understanding Email-Borne Viruses

1. Visit one or more of the antivirus software developer sites (Symantec, MacAfee, Computer Associates, Trend Micro, and so forth), and see if you can identify which viruses and worms require a user to click on an email attachment to replicate.
2. Trace the sophistication of the virus writers over time, and try to determine how they circumvent any improvements in user awareness of and education toward preventing viruses from spreading.

PROJECT 2.2: Researching Hackers

Open disclosure of software vulnerabilities is often associated with gray-hat hackers, described as security researchers who aren't particular about who learns about their findings. Research the three types of hackers (white hat, gray hat, and black hat), and try to determine their typical positions on full disclosure of software problems before patches or new versions of the software are made available in the marketplace. Use Google or your favorite Internet search engine with a query of "Open Disclosure of Software Vulnerabilities" to help you formulate your answers.

PROJECT 2.3: Comparing Physical and Virtual Risk-Management Techniques

1. How is risk management for physical systems similar to risk management for computer systems?
2. How are the two different?
3. What skill sets are required for each type?

This page intentionally left blank

Symbols

3DES (Triple DES), 207

2013 Computerworld Salary Survey website, 4

A

abstraction, 84

acceptable use sample policy, 306-308

definitions, 310

email/communications, 310

enforcement, 310

general use and ownership, 307

proprietary information, 307

purpose, 307

revision history, 310

scope, 307

system and network activities, 308-309

unacceptable use, 308

access controls

access control lists, 184

administrative, 149-150

authentication, 183

 fingerprint, 157-158

 headers (IPSec), 250

 multifactor, 188-189

 networks, 231

 overview, 183

 passwords, 186-189

 VPN, 317

- biometrics, 189-190
- controlled protection, 88
- coordinators, 9
- discretionary, 88, 184
- identification, 183
- information owners, 184
- key areas of knowledge, 292
- least privilege, 183
- logs, 155
- mandatory, 185
- matrix model, 102
- military classifications/clearances, 186
- networks, 232
- overview, 42
- physical, 149
 - alarm systems, 156
 - audit trails/access logs, 155
 - badging, 152
 - biometrics, 156-157
 - fingerprint authentication, 157-158
 - intrusion detection, 155
 - keys/combination locks, 152
 - lighting, 153
 - perimeters, 151
 - security dogs, 153
 - site selections, 150
 - smart cards, 153-155
 - visitors, 150
 - work area restrictions, 150
- remote, 192-193
- role-based, 185
- single sign-on, 190
 - federated identities, 192
 - Kerberos, 191
- users
 - access requests, 28
 - provisioning, 184
- account takeovers, 282**
- ACLs (access control lists), 184**
- Address Resolution Protocol (ARP), 230**
- administrative access controls, 149-150**
- administrative laws, 130**
- Advanced Research Projects Network (ARPANET), 229**
- Advanced Study of Information Warfare website, 129**
- AES (Advanced Encryption System), 207**
- agile software development, 262**
- alarm systems, 156**
- ALE (annualized loss expectancy), 70**
- alternate-site services providers, 116-117**
- Amazon.com "one click" software patent, 132**
- analysis**
 - business impact (BIA), 111, 114-115
 - risks, 26, 70-72
 - static, 269
- annualized loss expectancy (ALE), 70**
- appliances (network security), 241**
- Application Layer (OSI), 227**
- application-level gateway firewalls, 239-241**
 - bastion hosts, 239-240
 - benefits, 240
 - costs, 238
 - defined, 238
 - limitations, 241
 - proxy server characteristics, 239
- architecture and design, 81**
 - assurance, 86
 - evaluation models, 87
 - Common Criteria. *See* CC
 - Common Evaluation Methodology Editorial Board, 100-101
 - CTCPEC, 93
 - Federal Criteria, 93
 - ITSEC, 91-93
 - TCSEC. *See* TCSEC

key areas of knowledge, 297

overview, 40

SDLC

deployment, 270-271

design reviews, 267

development, 268

testing, 270

threat modeling, 266-267

training, 272

security models, 101-102

TCB

defined, 81

protection mechanisms, 84-86

rings of trust, 81-84

ARP (Address Resolution Protocol), 230

ARPANET (Advanced Research Projects Network), 229

art theft, 19

asset classifications, 67-68

assurance, 86

evaluation

classes, 97-98

levels, 98-100

models. *See* evaluation models

goals, 86

requirements, 24

asymmetric keys, 206-208

attackers, 27

attacks

categories, 127

computer forensics, 135-136

DDoS, 128

DoS, 128

dumpster diving, 128

emanation eavesdropping, 129

embezzlement, 129

highly publicized instances, 129

information warfare, 129

laws

administrative, 130

intellectual property, 131-132

judicial, 130

legislative, 130

privacy, 133-135

network protection, 231-232

password cracking, 187

pedestrian methods, 129

phishing, 192

replay, 250

rogue code, 128

social engineering, 128

software piracy, 128

spoofing, 128

surfaces, 267

Verizon Data Breach, 127

victims, 127

audit trails, 155

authentication

fingerprint, 157-158

headers (IPSec), 250

multifactor, 188-189

networks, 231

overview, 183

passwords, 186

cracking, 187

creating, 188

tokens, 189

VPN, 317

availability, 21

awareness, 72

B

B2B (business-to-business) processing, 3

backups, 172

badging, 152

Barquin, Dr. Ramon C., 138

baselines, 66

basic packet-filtering, 236

bastion hosts, 239-240

BCPs (business continuity plans), 111

BIA, 111, 114-115

creating, 112

defined, 111

DRP

alternate-side services providers, 116-117

cloud, 118

goals, 115

mobile units, 118

multiple centers, 117

recovery strategies, 116

service bureaus, 118

shared-site agreements, 116

testing, 118-119

importance, 112-113

key areas of knowledge, 299

overview, 40

scope, 114

threats, identifying, 113-114

Bell, David E., 101

Bell Laboratories "Conversion of Numerical Information" patent website, 132

Bell-LaPadula model, 101

BIA (business impact analysis), 111, 114-115

Biba model, 102

biometrics, 157, 189-190

convenience and security balance, 157

defined, 156

fingerprint authentication, 157-158

block ciphers, 214

B-Rate safe rating, 19

breach trends, 284-285

BS (British Standard) 7777, 65

BSIMM (Building Security in Maturity Model), 272

buffer overflow vulnerabilities, 27

business-to-business (B2B) processing, 3

businesses

attacks, 127

confidential classification, 68

continuity plans. *See* BCPs

impact analysis (BIA), 111, 114-115

information security career support, 9-10

organization structure, 10

sensitive classification, 68

C

CABs (change advisory boards), 271

Caesar cipher, 206

Cain and Abel password-cracking tool, 187

Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), 87, 93

CANs (campus area networks), 233

carders, 282

careers

CBK

access control, 42, 292

architecture and design, 40, 297

business continuity and disaster recovery planning, 40, 299

cryptography, 42, 296-297

governance and risk management, 39, 294-295

legal regulations, investigations, and compliance, 41, 300

operations security, 42, 298

overview, 39

physical security, 41, 301

software development security, 43, 295

telecommunications and network security, 43, 293

certifications

benefits, 37-38

Certified Cyber Forensics Professional, 45

Certified Information Security Manager, 44

- Certified Information Systems Auditor, 44
- Certified in Risk and Information Systems Control, 44
- Global Information Assurance Certifications, 44
- HealthCare Information Security and Privacy Practitioner, 45
- (ISC)2 specialization, 45
 - vendor-specific, 46
- compliance/governance professionals, 10
- demand, 4
- education
 - Carnegie Mellon Master of Science in Information Security degrees, 4
 - Department of Homeland Security supported certificate programs, 6
 - multidisciplinary approaches, 7
 - popularity, 7
- (ISC)2, 38-39
- listing of, 9-10
- Carnegie Mellon Master of Science in Information Security, 4**
- CBK (Common Body of Knowledge), 36**
 - access control, 42, 292
 - architecture and design, 40, 297
 - business continuity and disaster recovery planning, 40, 299
 - cryptography, 42, 296-297
 - governance and risk management, 39, 294-295
 - legal regulations, investigations, and compliance, 41, 300
 - operations security, 42, 298
 - overview, 39
 - physical security, 41, 301
 - software development security, 43, 295
 - telecommunications and network security, 43, 293
- CC (Common Criteria), 94**
 - development, 94
 - Editorial Board (CCEB), 94
 - evaluation assurance
 - classes, 97-98
 - levels, 98-100
 - functional requirements classes, 96-97
 - packages, 95
 - Protection Profiles, 95-96
 - targets of evaluation, 95
 - website, 94
- CCEB (CC Editorial Board), 94**
- CCFP (Certified Cyber Forensics Professional), 45**
- CCNP Security (Cisco Certified Network Professional Security), 46**
- CCSK (Certificate of Cloud Security Knowledge), 46**
- CEH (Certified Ethical Hacker), 46**
- CEM (Common Evaluation Methodology), 100**
- CEMEB (Common Evaluation Methodology Editorial Board), 100-101**
- Certificate of Cloud Security Knowledge (CCSK), 46**
- certificates (digital), 212-214**
- certifications**
 - benefits, 37-38
 - CBK
 - access control, 42, 292
 - architecture and design, 40, 297
 - business continuity and disaster recovery planning, 40, 299
 - cryptography, 42, 296-297
 - governance and risk management, 39, 294-295
 - legal regulations, investigations, and compliance, 41, 300
 - operations security, 42, 298
 - overview, 39
 - physical security, 41, 301
 - software development security, 43, 295
 - telecommunications and network security, 43, 293

Certified Cyber Forensics Professional, 45
 Certified Information Security Manager, 44
 Certified Information Systems Auditor, 44
 Certified in Risk and Information Systems Control, 44
 Global Information Assurance Certifications, 44
 HealthCare Information Security and Privacy Practitioner, 45
 (ISC)2, 38-39, 45
 vendor-specific, 46
Certified Cyber Forensics Professional (CCFP), 45
Certified Ethical Hacker (CEH), 46
Certified Information Security Manager (CISM), 44
Certified Information Systems Auditor (CISA), 44
Certified Information Systems Security Professional. See CISSPs
Certified in Risk and Information Systems Control (CRISC), 44
Certified Secure Software Lifecycle Professional (CSSLP), 45
 chain emails, 311
 change advisory boards (CABs), 271
 change management controls, 168, 171
 Chief Information Officers website, 3
 Chief Information Security Officer (CISO), 73
 CIA (confidentiality, integrity, availability) triad, 20-21
 CIP (Critical Infrastructure Protection), 281
 CISA (Certified Information Systems Auditor), 44
 Cisco Certified Network Professional Security (CCNP Security), 46
 CISM (Certified Information Security Manager), 44
 CISO (Chief Information Security Officer), 73

CISSPs (Certified Information Systems Security Professionals), 36

Code of Ethics, 136-137
 concentrations, 45
 overview, 38

civil laws, 130

Clark and Wilson model, 102

classifications

assets/data, 67-68
 military, 186

clearances (military), 186

closed systems, 85

cloud computing, 118, 254

Cloud Security Alliance (CSA), 46, 254

CloudArray website, 118

COBIT (Control Objectives for Information and Related Technology), 65

Code of Ethics (ISC)2, 136-137

Code of Fair Information Practices, 139

codebooks, 202

cold sites, 117

college certificate programs, 6

combination cards, 154

combination locks (physical access), 152

commercial encryption controls website, 201

Common Body of Knowledge. See CBK

Common Criteria. See CC

Common Evaluation Methodology (CEM), 100

Common Evaluation Methodology Editorial Board (CEMEB), 100-101

common laws, 130

intellectual property, 131-132

privacy, 133

FTC electronic commerce practices, 133

international, 133-134

United States, 134-135

communications

acceptable use policy example, 310

covert channels, 102-103

- IPSec, 249-250
 - authentication headers, 250
 - Encapsulating Security Protocol, 251
 - integrity value check, 250
 - ISAKMP, 251-252
 - key management, 253
 - modes, 250
 - security associations, 251
 - security policies, 252
 - VPNs, 253
- OSI, 226
 - Application Layer, 227
 - Data Link Layer, 229
 - Network Layer, 228
 - overview, 226
 - Physical Layer, 229
 - Presentation Layer, 228
 - protection, 231-232
 - reference model, 227
 - Session Layer, 228
 - TCP/IP mapping, 229-231
 - Transport Layer, 228
- out-of-band, 252
- complexity, 29**
- compliance, 41**
 - HIPAA, 320
 - administrative procedures, 321
 - physical safeguards, 321
 - technical mechanisms/services, 322
 - key areas of knowledge, 300
 - professionals, 9-10
- Computer and Information Systems Managers career information website, 4**
- computer-based covert channels, 103**
- computer crimes**
 - categories, 127
 - DDoS attacks, 128
 - DoS attacks, 128
 - dumpster diving, 128

- emanation eavesdropping, 129
- embezzlement, 129
- ethics
 - Code of Fair Information Practices, 139
 - Internet Activities Board Ethics and the Internet standard, 138
 - (ISC)2 Code of Ethics, 136-137
 - Ten Commandments of Computer Ethics, 138
- forensics, 135-136
- highly publicized instances, 129
- information warfare, 129
- laws
 - administrative, 130
 - intellectual property, 131-132
 - judicial, 130
 - legislative, 130
 - privacy, 133-135
- pedestrian methods, 129
- rogue code, 128
- social engineering, 128
- software piracy, 128
- spoofing, 128
- Verizon Data Breach, 127
- victims, 127
- Computer Ethics Institute Ten Commandments of Computer Ethics, 138**
- computer forensics, 135-136**
- Computer Security Act, 134**
- Computerworld Magazine**
 - annual hiring forecast survey website, 10
 - salary survey (2013) website, 4
- confidential classification, 186**
- confidentiality. See also access controls**
 - Bell-LaPadula model, 101
 - least privilege, 183
 - models, 20
 - synonyms, 20
- confidentiality, integrity, availability (CIA) triad, 20**

configuration controls, 168, 171

consequences/likelihood matrix (risks), 26

contact smart cards, 154

contactless smart cards, 154

Continuity Central website, 113

continuity. *See* **BCPs**

Control Objectives for Information and Related Technology (COBIT), 65

controls

- detection, 27
- dual, 29
- people, 29
- prevention, 27
- process, 29
- protection, 84-86
- responsive, 27
- risk analysis, 71
- technology, 29

covert channels, 102-103

cracking passwords, 187

C-Rate safe rating, 19

credit card fraud, 282

criminal laws, 131

CRISC (Certified in Risk and Information Systems Control), 44

Critical Infrastructure Protection (CIP), 281

cryptography, 201

- codebooks, 202
- digest-creation techniques, 209
- digital
 - block ciphers, 214
 - certificates, 212-214
 - hashing functions, 214
 - PPK implementation, 215-217
 - signatures, 209-210
- history, 201
- key areas of knowledge, 296-297

- keys, 206
 - asymmetric, 208
 - Identification Friend or Foe (IFF) System, 208
 - symmetric, 207
 - types, 206
- NSA, 201
- overview, 42
- plain text, 202
- random number requirements, 203
- Secure Hashing Algorithm, 210
- strength, 203
- substitution ciphers, 206
- telegraphs, 202
- terminology, 201
- transposition encryption example, 203-205

cryptosystems, 203

CSA (Cloud Security Alliance), 46, 254

CSSLP (Certified Secure Software Lifecycle Professional), 45

CTCPEC (Canadian Trusted Computer Product Evaluation Criteria), 87, 93

custodians of information resources, 73

customer confidential classification, 68

cyber forensics, 45

cybercrimes

- breach trends, 284-285
- carders, 282
- definitions, 282
- phishing, 283
- spear phishing, 283
- Stuxnet worm, 284
- Zeus Banking Trojan, 282-283

D

DAC (discretionary access control), 184

data

- backups, 172
- classifications, 67-68

- confidentiality, 232
- encryption standard (DES), 207
- flow stack, 227-229
- hiding, 84
- integrity, 232
- labels, 89

Data Link Layer (OSI), 229

DDoS (Distributed Denial of Service) attacks, 128

decryption keys, 206

- asymmetric, 208
- Identification Friend or Foe (IFF) System, 208
- public-private. *See* PPK
- symmetric, 207
- types, 206

de facto policies, 65

defense in depth

- defined, 22
- dual controls, 29
- networks
 - basic security infrastructures, 235
 - firewalls. *See* firewalls
 - IDSs, 245-248
 - IPSS, 248
 - routers, 236-237
- physical access controls
 - badging, 152
 - keys/combination locks, 152
 - lighting, 153
 - perimeters, 151
 - security dogs, 153
- process controls, 29
- technology controls, 29

degaussing, 174

de jure policies, 65

demilitarized zone (DMZ) networks, 243

Denial of Service (DoS) attacks, 128

Department of Defense. *See* DOD

Department of Homeland Security supported certificate programs, 6

deployment (software), 270-271

DES (Data Encryption Standard), 207

design. *See* architecture and design

destroying media, 174

detection controls, 27

development

- Common Criteria, 94
- policies, 62-63
- software. *See* SDLC

development phase (SDLC), 268-269

digital cryptography

- block ciphers, 214
- certificates, 212-214
- hashing functions, 214
- PPK implementation, 215
 - PGP, 216
 - SET, 217
 - S/MIME, 217
 - SSL, 215
 - TLS, 216
- signatures, 209-210

digital signatures, 232

disaster recovery planning. *See* DRP

discretionary access control (DAC), 184

discretionary protection, 88

disposing, media, 173-174

Distributed Denial of Service (DDoS) attacks, 128

Division A (TCSEC), 90-91

Division B (TCSEC), 88-90

Division C (TCSEC), 88

Division D (TCSEC), 88

DMZ (demilitarized zone) networks, 243

documenting policies, 63

- guidelines, 67
- procedures, 67
- regulations, 64-66
- standards and baselines, 66

DOD (Department of Defense)

- ARPANET, 229

- security clearances, 70

- TEMPEST program, 129

dogs (security), 153**domain protections, 89****DoS (Denial of Service) attacks, 128****DRP (disaster recovery planning)**

- alternate-site services providers, 116-117

- cloud, 118

- defined, 111

- goals, 115

- history, 111

- mobile units, 118

- multiple centers, 117

- overview, 40

- service bureaus, 118

- shared-site agreements, 116

- strategies, identifying, 116

- testing, 118-119

dual controls, 29**duties, separating, 68-69****E****EALs (Evaluation Assurance Levels), 98-100****education. See also certifications**

- Carnegie Mellon Master of Science in Information Security degrees, 4

- Department of Homeland Security supported certificate programs, 6

- multidisciplinary approaches, 7

Electronic Communications Act, 134**email, 310-312****emanation eavesdropping, 129****embezzlement, 129****employee screenings, 69****Encapsulating Security Protocol (ESP), 251****encipherment, 232****encryption**

- keys, 206

- asymmetric, 208

- Identification Friend or Foe (IFF) System, 208

- public-private. *See* PPK

- symmetric, 207

- types, 206

- transposition example, 203-205

- VPN, 317

enforcement, 310**environmental security. See physical security****ESP (Encapsulating Security Protocol), 251****ethical hackers, 46****ethics**

- Code of Fair Information Practices, 139

- Internet Activities Board Ethics and the Internet standard, 138

- (ISC)2 Code of Ethics, 136-137

- Ten Commandments of Computer Ethics, 138

European Information Technology Security Evaluation Criteria. See ITSEC**evaluation models, 87**

- Common Criteria, 94

- development, 94

- Editorial Board (CCEB), 94

- evaluation assurance classes, 97-98

- evaluation assurance levels, 98-100

- functional requirements classes, 96-97

- packages, 95

- Protection Profiles, 95-96

- targets of evaluation, 95

- website, 94

- Common Evaluation Methodology Editorial Board, 100-101

- CTCPEC, 93

- Federal Criteria, 93

- ITSEC, 91

- assurance classes, 92-93

- TCSEC, compared, 91

TCSEC

Division A, 90-91

Division B, 88-90

Division C, 88

Division D, 88

European version. *See* ITSEC

ITSEC, compared, 91

overview, 87

TNI, 91

exploits, 27**extranets, 234****F****facility controls**

access

badging, 152

keys/combination locks, 152

lighting, 153

perimeters, 151

security dogs, 153

site selections, 150

visitors, 150

work area restrictions, 150

environmental/life safety, 158-159

technical

alarm systems, 156

audit trails/access logs, 155

biometrics, 156-157

fingerprint authentication, 157-158

intrusion detection, 155

smart cards, 153-155

fail-secure system controls, 168**Fair Credit Reporting Act, 134****Fair Debt Collection Practices Act, 135****false negative errors (IDSs), 248****false positive errors (IDSs), 247****fastest growing occupations website, 4****FC (Federal Criteria) for Information Technology Security, 87, 93****fear, uncertainty, and doubt (FUD), 29****Federal Information Security Management Act, 135****Federal Trade Commission (FTC), 133****federated identities, 192****FFIEC (Federal Financial Institutions Examination Council), 64****File Transfer Protocol (FTP), 231****financial cybercrimes, 128**

breach trends, 284-285

carders, 282

definitions, 282

phishing, 283

spear phishing, 283

ZeuS Banking Trojan, 282-283

Financial Services ISACs, 281**fingerprint authentication, 157-158****finite-state machines, 85****FIPS (Federal Information Processing Standard), 207****fire detection/suppression controls, 158-159****firewalls, 237**

application-level gateway, 239-241

bastion hosts, 239-240

benefits, 240

costs, 238

defined, 238

limitations, 241

proxy server characteristics, 239

choosing, 245

demilitarized zone, 243

homing, 238

packet-filtering, 241-242

screened host, 242-243

screened-subnet, 244

foreign nationals, 150**forensics, 135-136****forwarded emails, 311****FS-ISACs (Financial Services-Information Sharing and Analysis Centers), 281**

FTC (Federal Trade Commission), 133

FTP (File Transfer Protocol), 231

FUD (fear, uncertainty, and doubt), 29

functional decomposition, 267

functional requirements, 24, 96-97

G

George Washington University in Washington, D.C. certificate programs, 6

GIACs (Global Information Assurance Certifications), 44

GLBA (Gramm-Leach-Bliley Act), 68

governance

HIPAA

administrative procedures, 321

compliance, 320

enforcement, 68

overview, 65

physical safeguards, 321

technical mechanisms/services, 322

WLANs, 60-61

key areas of knowledge, 294-295

managers, 10

overview, 39

policies

de facto/de jure, 65

documenting, 63

effective, 55

guidelines, 67

implementation, 63

issue-specific, 60

operations, 63

overview, 55

procedures, 67

programme-framework, 59

programme-level, 57-59

publishing, 55

regulations, 64-66

security objectives, 62

standards and baselines, 66

structure, 55

system-specific, 61

tools, 55

types, 57

responsibilities, 73

standards

asset and data classification, 67-68

hiring practices, 69-70

risk analysis, 70-72

separation of duties, 68-69

user education/training/awareness, 72

Gramm-Leach-Bliley Act (GLBA), 68

grudge attacks, 128

H

hardware segmentation, 84

hashing functions, 214

HCISPP (HealthCare Information Security and Privacy Practitioner), 45

healthcare

HealthCare Information Security and Privacy Practitioner (HCISPP), 45

HIPAA

administrative procedures, 321

compliance, 320

enforcement, 68

overview, 65

physical safeguards, 321

technical mechanisms/services, 322

WLANs, 60-61

WLAN security, 60-61

heating, ventilation, and air conditioning (HVAC) controls, 159

hiding data, 84

hierarchy, 83

HIPAA (Health Insurance Portability and Accountability Act of 1996), 65, 135

administrative procedures, 321

compliance, 320

- enforcement, 68
- overview, 65
- physical safeguards, 321
- technical mechanisms/services, 322
- WLANs, 60-61

hiring practices, 69-70

homing, 238

hot sites, 116

human covert channels, 103

HVAC (heating, ventilation, and air conditioning) controls, 159

I

ICMP (Internet Control Message Protocol), 231

identification

- authentication, 183
 - fingerprint, 157-158
 - headers (IPSec), 250
 - multifactor, 188-189
 - networks, 231
 - overview, 183
 - passwords, 186-189
 - VPN, 317
- biometrics, 189-190
- credentials, 183
- Friend or Foe (IFF) System, 208

identity theft, 282

IDs (users), 169

IDSs (intrusion detection systems), 245-246

- false negative errors, 248
- false positive errors, 247
- good characteristics, 247
- intrusions, defined, 246-247
- subversion errors, 248

IETF (Internet Engineering Task Force), 249

IFF (Identification Friend or Foe) System, 208

incident response team members, 9

information

- flow model, 102
- owners, 184
- resources managers, 73
- storage, 84
- warfare attacks, 129

Information Sharing and Analysis Centers (ISACs), 281

Information Technology Security Evaluation Criteria (ITSEC), 87

InfoSec

- organization structure, 10
- professionals future, 285
- umbrella, 7

integrity. See also access control

- Biba model, 102
- models, 21
- value check (IVC), 250
- verification, 173

intellectual property law, 131-132

intelligence attacks, 127

interdependencies (operations), 175-176

internal auditors, 73

International Information Systems Security Certifications Consortium. See (ISC)2

international privacy laws, 133-134

International Safe Harbor Principles, 134

Internet, 233

- Activities Board Ethics and the Internet standard, 138
- Assigned Numbers Authority, 230
- Control Message Protocol (ICMP), 231
- Engineering Task (IETF), 249
- Protocol (IP), 230
- Protocol address spoofing, 128
- Security Association and Key Management Protocol (ISAKMP), 251-252
- as store-and-forward network, 234

intranets, 234

intrusion detection systems. See IDSs

intrusions, 246-247

investigations, 41, 300

IP (Internet Protocol), 230

IP address spoofing, 128

IPSec, 249-250

authentication headers, 250

Encapsulating Security Protocol, 251

integrity value check, 250

ISAKMP, 251-252

key management, 253

modes, 250

security

associations, 251

policies, 252

VPNs, 253

IPs (intrusion prevention systems), 248

ISACs (Information Sharing and Analysis Centers), 281

ISAKMP (Internet Security Association and Key Management Protocol), 251-252

(ISC)2 (International Information Systems Security Certification Consortium)

CBK

access control, 42, 292

architecture and design, 40, 297

business continuity and disaster recovery planning, 40, 299

cryptography, 42, 296-297

governance and risk management, 39, 294-295

legal regulations, investigations, and compliance, 41, 300

operations security, 42, 298

overview, 39

physical security, 41, 301

software development security, 43, 295

telecommunications and network security, 43, 293

certification benefits, 37-38

Code of Ethics, 136-137

goals, 38

primary designations, 38

specialization certificates, 45

website, 39

ISO/IEC, 39

ISO/IEC "Code of Practice for Information Security Management," 65, 302-304

issue-specific policies, 60

IT job demand website, 285

ITSEC (Information Technology Security Evaluation Criteria), 87

assurance classes, 92-93

TCSEC, compared, 91

IVC (integrity value check), 250

J

John the Ripper, 187

judicial laws. See common laws

K

Kennedy-Kassenbaum Health Insurance and Portability Accountability Act. See HIPAA

Kerberos, 191

keys, 206

asymmetric, 208

Identification Friend or Foe (IFF) System, 208

IPSec management, 253

public/private. *See* PPK

symmetric, 207

types, 206

keys (physical access), 152

Krebs on Security website, 285

L

labeling data/media, 89, 172

LANs (Local Area Networks), 233

LaPadula, Leonard J., 101**laws**

- administrative, 130
- common, 130
- intellectual property, 131-132
- legislative, 130
- privacy, 133
 - FTC electronic commerce practices, 133
 - international, 133-134
 - United States, 134-135

layered security. *See* defense in depth

layering, 84

least privilege, 183

legal regulations, 41, 300

legislative laws, 130

life safety controls, 158-159

lighting, 153

Local Area Networks (LANs), 233

logging

- media, 172
- networks, 232

M

MAC (mandatory access control), 185

maintenance, 174-175

man made disaster events, 113

mandatory protection, 88-90

MANs (metropolitan area networks), 233

mantraps, 152

marking media, 172

Mary, Queen of Scots (cryptography), 202

Master of Science in Information Security (Carnegie Mellon), 4

maturity measurement models (software), 272

media controls, 172

- disposition, 173-174
- environmental protection, 173
- integrity verification, 173
- logging, 172

marking/labeling, 172

physical access protection, 173

transmittal, 173

viability, 169

memory cards, 154

metropolitan area networks (MANs), 233

military

- attacks, 127
- classifications/clearances, 70, 186

minimal protection, 88

mitigation planning, 267

mobile units, 118

monitoring networks, 232

Monroe Community College in Rochester, New York degree programs, 6

motion detectors, 156

Multics (Multiplexed Information and Computing Service), 82

multidisciplinary education approaches, 7

multifactor authentication, 188-189

multihomed firewalls, 238

multiple center arrangements, 117

Multiplexed Information and Computing Service (Multics), 82

multiprogramming systems, 85

multitasking, 85

music piracy, 131

N

NAT (network address translation), 245

National Council of ISACs, 281

National Retail Security Survey (NRSS), 147

National Security Agency (NSA), 201

National Security Directive 42 (NSD-42), 135

National Training Standard for Information Systems Security Professionals, 65

natural disaster events, 113

natural justice, 130

Naval Postgraduate School for Homeland Defense and Security, 6

NDCI (National Data Conversion Institute), 136

NetIQ website, 55

network address translation (NAT), 245

Network Layer (OSI), 228

networks

acceptable use policy example, 308-309

access control, 232

authentication, 231

basic security infrastructures, 235

cloud, 254

data confidentiality, 232

data integrity, 232

extranets, 234

firewalls, 237

application-level gateway, 238-241

choosing, 245

demilitarized zone, 243

homing, 238

packet-filtering, 241-242

screened host, 242-243

screened-subnet, 244

IDSs, 245-246

false negative errors, 248

false positive errors, 247

good characteristics, 247

intrusions, defined, 246-247

subversion errors, 248

Internet. *See* Internet

intranets, 234

IPSec, 249-250

authentication headers, 250

Encapsulating Security Protocol, 251

integrity value check, 250

ISAKMP, 251-252

key management, 253

modes, 250

security associations, 251

security policies, 252

VPNs, 253

IPs, 248

key areas of knowledge, 293

LANs, 233

logging/monitoring, 232

NAT, 245

nonrepudiation, 232

OSI. *See* OSI

out-of-band communications, 252

overview, 43

protecting from attacks, 231-232

rings of trust, 83

routers, 236-237

security appliances, 241

VPNs

IPSec-based, 253

overview, 249

WANs, 233

wireless (WiFi), 317-318

NFRs (nonfunctional requirements), 265

Nilson Report website, 284

noninterference model, 102

nonrepudiation, 232

Northeastern University in Boston degree programs, 6

notarization, 232

NRSS (National Retail Security Survey), 147

NSA (National Security Agency), 201

NSD-42 (National Security Directive 42), 135

NSTISSC (National Security Telecommunications and Information Systems Security Committee) Standard 4011, 65

O

Oakley Key Determination Protocol, 252

Ohio State University degree programs, 6

one-time passwords (OTPs), 189

Open PGP, 217

open systems, 85

Open Systems Interconnection. See OSI

Open Web Application Security Project. See OWASP

OpenSAMM (Open Software Assurance Maturity Model), 272

Operation Eligible Receiver, 281

operations

- backups, 172
- configuration and change management, 171
- documentation, 174
- interdependencies, 175-176
- key areas of knowledge, 298
- maintenance, 174-175
- media controls, 172
 - disposition, 173-174
 - environmental protection, 173
 - integrity verification, 173
 - logging, 172
 - marking/labeling, 172
 - physical access protection, 173
 - transmittal, 173
- overview, 42
- process controls, 168-169
- separation of duties, 167-168
- software support, 171

organization structure, 10

OSI (Open Systems Interconnection), 226

- ISO security services, 231-232
- layers
 - Application, 227
 - Data Link, 229
 - Network, 228
 - Physical, 229
 - Presentation, 228
 - reference model, 227
 - Session, 228
 - Transport, 228
- overview, 226
- TCP/IP mapping, 229-231

OTPs (one-time passwords), 189

out-of-band communications, 252

overwriting, 174

OWASP (Open Web Application Security Project), 268

OpenSAMM, 272

Top Ten, 268

owners of information resources, 73

P

packet filtering, 236-237

- basic, 236
- benefits, 236
- firewalls, 241-242
- limitations, 237
- stateful inspection, 236

Password Safe website, 190

passwords

- cracking, 187
- creating, 188
- problems, 186
- sample policy, 312-316
 - application development, 315
 - creating, 313-314
 - definitions, 316
 - enforcement, 316
 - general, 313
 - passphrases, 316
 - protection standards, 314-315
 - purpose, 312
 - remote access, 316
 - scope, 312
- strong, 314
- tokens, 189
- vault, creating, 190
- weak, 314

Patent and Trademark Office (PTO), 131

patents, 131

Patriot Act HR 3162, 135

PDD (Presidential Decision Directive) 63, 281

Peeler, Julie, 285

peer reviews (software development), 269

people controls, 29

people, process, and technology triad, 29

perfect forward secrecy (PFS), 252

perimeter intrusion and detection assessment system (PIDAS), 151

perimeter security controls, 151, 156

personnel

controls, 169

education, 149

PFS (perfect forward secrecy), 252

PGP (Pretty Good Privacy), 216

phishing, 23, 192

financial crimes, 283

preventing, 23

Physical Layer (OSI), 229

physical security, 41

access controls, 149-150

badging, 152

educating personnel, 149

environmental/life safety, 158-159

goal, 147

key areas of knowledge, 301

keys/combination locks, 152

lighting, 153

media protection, 173

overview, 147

perimeters, 151

security dogs, 153

technical

alarm systems, 156

audit trails/access logs, 155

biometrics, 156-157

fingerprint authentication, 157-158

intrusion detection, 155

smart cards, 153-155

threats, 148

PIDAS (perimeter intrusion and detection assessment system), 151

PIN vaults, creating, 190

PKI (public key infrastructures), 206-208

plain text, 202

policies

de facto/de jure, 65

developing, 62-63

effective, 55

outline, 302-304

overview, 55

publishing, 55

standards

asset and data classification, 67-68

hiring practices, 69-70

risk analysis, 70-72

separation of duties, 68-69

user education/training/awareness, 72

structure, 55

supporting documents

guidelines, 67

procedures, 67

regulations, 64-66

standards and baselines, 66

tools, 55

types, 57

issue-specific, 60

programme-framework, 59

programme-level, 57-59

system-specific, 61

policymakers, 9

power controls, 158

PPs (Protection Profiles), 95-96

PPK (public-private key cryptography), 215

digital certificates, 212-214

digital signatures, 209-212

implementations, 215

PGP, 216

SET, 217

S/MIME, 217

SSL, 215

TLS, 216

Presentation Layer (OSI), 228

President Clinton, PDD63, 281

Presidential Decision Directive (PDD) 63, 281

Pretty Good Privacy (PGP), 216

privacy laws, 133

FTC electronic commerce practices, 133

international, 133-134

United States, 134-135

private keys. See PPK

privileged entity controls, 169

probability, calculating, 71

process controls, 29, 168

backups, 172

configuration and change management, 168, 171

documentation, 174

interdependencies, 175-176

maintenance, 174-175

media, 172

disposition, 173-174

environmental protection, 173

integrity verification, 173

logging, 172

marking/labeling, 172

physical access protection, 173

transmittal, 173

media viability, 169

personnel, 169

privileged entity controls, 169

record retention, 169

resource protection, 169

software support, 171

SOX, 169

trusted recovery, 168

programme-framework policies, 59

programme-level policies, 57-59

protection

discretionary, 88

mandatory, 88-90

minimal, 88

profiles (PPs), 95-96

structured, 89

TCB, 84-86

verified, 90-91

protocols

ARP, 230

ESP, 251

ICMP, 231

IP, 230

ISAKMP, 251-252

Kerberos, 191

Oakley Key Determination, 252

OSI stack

Application Layer, 227

Data Link Layer, 229

Network Layer, 228

overview, 226

Physical Layer, 229

Presentation Layer, 228

reference model, 227

Session Layer, 228

Transport Layer, 228

PGP, 216

RARP, 230

SET, 217

SKEP, 253

SKIP, 253

S/MIME, 217

SMTP, 231

SSL, 215

TCP, 230

TCP/IP

applications, 231

OSI model, mapping, 229-231

protocols, 230-231

TLS, 216

UDP, 230

provisioning users, 184

proxy servers, 239

PTO (Patent and Trademark Office), 131

public information classification, 68

public key infrastructures (PKI), 206-208

public-private key cryptography. *See* PPK

Q

qualitative risk analysis, 71-72

quantitative risk analysis, 70-71

Queen Elizabeth I plot (cryptography), 202

R

RADIUS (Remote Access Dial-In User Service), 193

random number requirements (cryptography), 203

RARP (Reverse Address Resolution Protocol), 230

ratings

risks, 26

safes, 19

RBAC (role-based access control), 185

record retention, 169

recovery planning. *See also* BCPs

alternate-site services providers, 116-117

cloud, 118

defined, 111

goals, 115

history, 111

identifying, 116

key areas of knowledge, 299

mobile units, 118

multiple centers, 117

service bureaus, 118

shared-site agreements, 116

testing, 118-119

regulatory laws, 131

remote access control, 192-193

Remote Access Dial-In User Service (RADIUS), 193

remote login (Telnet), 231

replay attacks, 250

requirements gathering and analysis phase (SDLC), 265-266

resource protection, 169

responsibilities, 73

responsive controls, 27

Reverse Address Resolution Protocol (RARP), 230

rings of trust, 81

implementing, 84

networks, 83

ring hierarchy, 83

stand-alone systems, 82

risks, 39

analysis

consequences/likelihood, 26

qualitative, 71-72

quantitative, 70-71

attackers, 27

exploits, 27

key area of knowledge, 294-295

outcomes, 25

vulnerabilities, 27

rogue code, 128

role-based access control (RBAC), 185

ROT13 cipher, 206

routers, 236-237

routing controls, 232

RSA Security 2011 breach website, 192

S

Safe Harbor Privacy Principles, 134

safe ratings, 19

SANS Security Policy Project

- acceptable use, 306-308
 - definitions, 310
 - email/communications, 310
 - enforcement, 310
 - general use and ownership, 307
 - proprietary information, 307
 - purpose, 307
 - revision history, 310
 - scope, 307
 - system/network activities, 308-309
 - unacceptable use, 308

- email, 310-312

- passwords, 312-316

- application development, 315

- creating, 313-314

- definitions, 316

- enforcement, 316

- general, 313

- passphrases, 316

- protection standards, 314-315

- purpose, 312

- remote access, 316

- scope, 312

- website, 306

- WiFi, 317-318

SAP (special access programs), 186**Sarbanes-Oxley Corporate Responsibility and Accountability Act (SOX), 64, 169****SAs (security associations), 251****SCI (sensitive compartmented information), 186****screened host firewalls, 242-243****screened-subnet firewalls, 244****Scrum software methodology, 262****SDLC (Software Development Life Cycle), 263**

- built-in security, 263-264

- deployment, 270-271

- design reviews, 267

- development, 268-269

- key areas of knowledge, 295

- maturity measurement models, 272

- phases, 263

- requirements gathering and analysis, 265-266

- security overview, 265

- testing, 270

- threat modeling, 266-267

- training, 272

Search Security Magazine information security career popularity, 7**SEC (Securities and Exchange Commission), 64****secret classification, 186****Secure Electronic Transactions (SET), 217****Secure Hash Algorithm (SHA), 210****Secure/Multipurpose Internet Mail Extensions (S/MIME), 217****Secure Sockets Layer (SSL), 215****security**

- administrators, 9

- architects, 9

- associations (SAs), 251

- consultants, 9

- dogs, 153

- models, 101-102

- policy database (SPD), 252

- policy project. *See* SANS Security Policy Project

- testers, 9

- through obscurity, 25

sensitive compartmented information (SCI), 186**sensitive information emails, 311****separation of duties, 29, 167**

- benefits, 167

- importance, 167

- production operations, 168

- standards, 68-69

servers, 239

service bureaus, 118

Service Organization Controls, 170

Service Set Identifier (SSID), 317

session laws. See statutory laws

Session Layer (OSI), 228

SET (Secure Electronic Transactions), 217

SHA (Secure Hash Algorithm), 210

SHA-3 Cryptographic Hash Algorithm Competition, 210

shared-site agreements, 116

signatures (digital), 209-210

single-homed firewalls, 238

single sign-on. See SSO

site access controls. See facility controls

SKEP (Simple Key Exchange Protocol), 253

SKIP (Simple Key Interchange Protocol), 253

smart cards, 153-155

S/MIME (Secure/Multipurpose Internet Mail Extensions), 217

SMTP (Simple Mail Transfer Protocol), 231

social engineering, 128

software

agile development, 262

attack surfaces, 267

backups, 172

development life cycle (SDLC)

built-in security, 263-264

deployment, 270-271

design reviews, 267

development, 268-269

key areas of knowledge, 295

maturity measurement models, 272

phases, 263

requirements gathering and analysis, 265-266

security overview, 265

testing, 270

threat modeling, 266-267

training, 272

maturity measurement models, 272

piracy, 128

quality, 261

spaghetti code, 262

support, 171

writing, 261

something you have plus something you know plus something you are (SYH/SYK/SYA), 189

something you have plus something you know (SYH/SYK), 188

SOX (Sarbanes-Oxley) Act, 64, 169

spaghetti code, 262

SPD (security policy database), 252

spear phishing, 283

special access programs (SAP), 186

spoofing, 128

SSAE 16 (Statement on Standards for Attestation Engagements), 170

SSCP (Systems Security Certified Practitioner), 36-38

SSID (Service Set Identifier), 317

SSL (Secure Sockets Layer), 215

SSO (single sign-on), 190

federated identities, 192

Kerberos, 191

standards

asset and data classification, 67-68

developers, 9

hiring practices, 69-70

outline, 302-304

policy support, 66

risk analysis, 70-72

qualitative, 71-72

quantitative, 70-71

separation of duties, 68-69

user education/training/awareness, 72

state machine model, 102

stateful inspection packet-filtering, 236

Statement on Standards for Attestation Engagements (SSAE), 16, 170

static analysis, 269

statutory laws, 130

storage, 84

straight packet-filtering, 236

strong passwords, 314

structured protections, 89

Stuxnet worm, 284

substitution ciphers, 206

subversion errors (IDSs), 248

SYH/SYK (something you have plus something you know), 188**SYH/SYK/SYA (something you have plus something you know plus something you are), 189**

symmetric keys, 206-207

system-specific policies, 61

Systems Security Certified Practitioner (SSCP), 36-38**T****Target Corporation breach, 284****targets of evaluation (TOE), 95****TCB (Trusted Computing Base), 81**

defined, 81

protections

discretionary, 88

mandatory, 88-90

mechanisms, 84-86

minimal, 88

verified, 90-91

rings of trust, 81

implementing, 84

networks, 83

ring hierarchy, 83

stand-alone systems, 82

TCP (Transmission Control Protocol), 230**TCP/IP (Transmission Control Protocol/Internet Protocol)**

applications, 231

OSI model, mapping, 229-231

protocols, 230-231

TCSEC (Trusted Computer System Evaluation Criteria)

Division A, 90-91

Division B, 88-90

Division C, 88

Division D, 88

European version. *See* ITSEC

ITSEC, compared, 91

overview, 87

TNI, 91

technical access controls

alarm systems, 156

audit trails/access logs, 155

biometrics, 156-157

fingerprint authentication, 157-158

intrusion detection, 155

smart cards, 153-155

technical managers, 73**technology controls, 29****telecommunications**

key areas of knowledge, 293

overview, 43

telegraphs, 202**Telnet (remote login), 231****TEMPEST program, 129****Ten Commandments of Computer Ethics, 138****terrorist attacks, 128****testing**

DRP, 118-119

goals, 86

models, 91

safe ratings, 19

software, 270

unit, 269

threats

- breach trends, 284-285
- carders, 282
- categorizing, 267
- disposed media, 174
- identifying, 113-114
- man made, 113
- modeling (SDLC), 266-267
- natural, 113
- OWASP Top Ten, 268
- password cracking, 187
- phishing, 192, 283
- physical security, 148
- ranking, 267
- risk analysis, 71
- spear phishing, 283
- Stuxnet worm, 284
- ZeuS Banking Trojan, 282-283

three-factor authentication, 189**thrill attacks, 128****TJX Corporation breach, 284****TLS (Transport Layer Security), 216****TNI (Trusted Network Interpretation), 91****TOE (targets of evaluation), 95****tokens (passwords), 189****tools**

- password-cracking, 187
- policies, 55

top secret classification, 186**trade secrets, 68, 132****trademarks, 132****traffic padding, 232****training**

- software development, 272
- users/personnel, 72, 149

Transmission Control Protocol (TCP), 230**Transmission Control Protocol/Internet Protocol. See TCP/IP****transmitting media, 173****Transport Layer (OSI), 228****Transport Layer Security (TLS), 216****transposition encryption example, 203-205****Triple DES (3DES), 207****Trusted Computer System Evaluation Criteria. See TCSEC****Trusted Computing Base (TCB), 81****Trusted Network Interpretation (TNI), 91****trusted recovery controls, 168****TwinStrata CloudArray website, 118****two-factor authentication, 188**

U**UDP (User Datagram Protocol), 230****UL (Underwriters Laboratory) TL-15 safe rating, 19****UL (Underwriters Laboratory) TL-30 safe rating, 20****umbrella (InfoSec), 7****unauthorized disclosure emails, 312****unit testing, 269****United States****Department of Defense****ARPANET, 229****security clearances, 70****TEMPEST program, 129****Department of Health and Human Services****Code of Fair Information Practices, 139****government****classification labels, 186****information system vulnerability demonstration, 281****laws, 130****National Security Agency, 201****National Security Telecommunications and Information Systems Security Committee (NSTISSC) Standard 4011, 65****privacy laws, 134-135****University of Houston Security Manual website, 73**

USA PATRIOT ACT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 135

User Datagram Protocol (UDP), 230

users

- access control. *See* access controls
- access requests, 28
- authentication, 183
 - fingerprint, 157-158
 - headers (IPSec), 250
 - multifactor, 188-189
 - networks, 231
 - overview, 183
 - passwords, 186-189
 - VPN, 317
- bad security decisions, 24
- education/training/awareness, 72
- IDs, 169
- identification, 183
- information owners, 184
- least privilege, 183
- provisioning, 184
- responsibilities, 73

V

vendor managers, 10

vendor-specific certification programs, 46

verification

- integrity, 173
- protections, 90-91

Verizon Data Breach, 127

virus warning emails, 312

visitor controls, 150

VPNs (virtual private networks), 193, 249

- encryption/authentication, 317
- IPSec-based, 253
- overview, 249

vulnerabilities

- defined, 27
- disclosing, 28
- open disclosure, 30
- Operation Eligible Receiver, 281
- OWASP Top Ten, 268
- risk analysis, 71

W

WANs (Wide Area Networks), 233

warm sites, 117

weak passwords, 314

websites

- 2013 Computerworld Salary Survey, 4
- Advanced Study of Information Warfare, 129
- Amazon.com book ordering patents, 132
- Bell Laboratories "Conversion of Numerical Information" patent, 132
- Carnegie, 4
- CCNP Security certificate, 46
- Certificate of Cloud Security Knowledge, 46
- Chief Information Officers, 3
- The Cloud Security Alliance, 254
- CloudArray, 118
- Code of Fair Information Practices, 139
- commercial encryption controls, 201
- Common Criteria, 94
- Computer and Information Systems Managers career information, 4
- Computerworld Magazine annual hiring forecast survey, 10
- Continuity Central, 113
- ethical hackers, 46
- fastest growing occupations, 4
- Financial Services ISACs, 281
- FTC electronic commerce privacy practices, 133
- GIAC certifications, 44
- Identification Friend or Foe (IFF) System, 208

Internet

- Activities Board Ethics and the Internet standard, 139
- Assigned Numbers Authority, 230
- (ISC)2, 39
- ISO/IEC, 39
- ISO/IEC 17799, “Code of Practice for Information Security Management,” 65
- IT job demand, 285
- Krebs on Security, 285
- music piracy, 131
- NAT, 245
- National Council of ISACs, 281
- Naval Postgraduate School for Homeland Defense and Security, 6
- NetIQ, 55
- Nilson Report, 284
- NRSS, 147
- NSTISSC Number 4011, 66
- OWASP Top Ten, 268
- password-cracking tools, 187
- password/PIN vaults, creating, 190
- Password Safe, 190
- Patent and Trademark Office, 131
- RBAC, 185
- RSA Security 2011 breach, 192
- SANS Security Policy Project, 306
- Scrum Alliance, 262
- Search Security Magazine information security career popularity, 7
- Secure Hash Standard, 210
- SHA-3 Cryptographic Hash Algorithm Competition, 210
- SSAE 16, 170
- Stuxnet worm, 284
- Ten Commandments of Computer Ethics, 138
- TJX Corporation breach, 284
- TNI, 91
- University of Houston Security Manual, 73

- U.S. government classification labels, 186
- vendor-specific certification programs, 46
- Verizon Data Breach, 127
- ZeuS Banking Trojan, 283

Whitworth Gallery art theft, 19**Wide Area Networks (WANs), 233****WiFi (wireless networks), 317-318**

- access points/cards registration, 317
- approved technology, 317
- definitions, 318
- enforcement, 318
- scope, 317
- SSID, 317
- VPN encryption/authentication, 317

WLANS, healthcare security, 60-61**work area controls, 150****writing software, 261**

X – Z**X.509 digital certificate standard, 212****Zimmerman, Phil, 216**