

Save 10%
on Exam
Voucher

See Inside

EXAM ✓ CRAM

CompTIA[®] **Security+** SY0-701



Exam Alerts



Cram
Sheet



Flash
Cards



Practice
Tests



ROBERT SHIMONSKI
MARTY M. WEISS

FREE SAMPLE CHAPTER |



CompTIA® Security+ SY0-701 Exam Cram

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, Key Term flash card application, the essential Cram Sheet, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonitcertification.com/register.
2. Enter the **print book ISBN**: 9780138225575.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to pearsonitp.ehelp.org.

This page intentionally left blank

EXAM ✓ **CRAM**

**CompTIA[®]
Security+
SY0-701
Exam Cram**

**Robert Shimonski
Marty M. Weiss**

CompTIA® Security+ SY0-701 Exam Cram

Robert Shimonski and Marty M. Weiss

Copyright © 2025 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

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.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose all such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

ISBN-13: 978-0-13-822557-5

ISBN-10: 0-13-822557-5

Library of Congress Cataloging-in-Publication Data: 2024909527

\$PrintCode

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 intlcs@pearson.com.

GM K12, Early Career and Professional Learning

Soo Kang

Director, ITP Product Management

Brett Bartow

Executive Editor

Nancy Davis

Development Editor

Ellie C. Bru

Managing Editor

Sandra Schroeder

Senior Project Editor

Mandie Frank

Copy Editor

Bart Reed

Indexer

Erika Millen

Proofreader

Jennifer Hinchliffe

Technical Editors

Raymond Lacoste
Christopher Crayton

Publishing Coordinator

Cindy Teeters

Designer

Chuti Prasertsith

Composer

codeMantra

Contents at a Glance

Introduction	xxvi
Part 1: General Security Concepts	1
CHAPTER 1 Security Controls	3
CHAPTER 2 Fundamental Security Concepts	11
CHAPTER 3 Change Management Processes and the Impact to Security	27
CHAPTER 4 Cryptographic Solutions	39
Part 2: Threats, Vulnerabilities, and Mitigations	81
CHAPTER 5 Threat Actors and Motivations	83
CHAPTER 6 Threat Vectors and Attack Surfaces	97
CHAPTER 7 Vulnerability Types	115
CHAPTER 8 Malicious Attacks and Indicators	131
CHAPTER 9 Mitigation Techniques for Securing the Enterprise	161
Part 3: Security Architecture	177
CHAPTER 10 Security Implications of Architecture Models	179
CHAPTER 11 Enterprise Architecture Security Principles	211
CHAPTER 12 Data Protection Strategies	233
CHAPTER 13 Resilience and Recovery in Security Architecture	247
Part 4: Security Operations	265
CHAPTER 14 Securing Resources	267
CHAPTER 15 Hardware, Software, and Data Asset Management	295
CHAPTER 16 Vulnerability Management	307
CHAPTER 17 Security Alerting and Monitoring	329
CHAPTER 18 Enterprise Security Capabilities	349
CHAPTER 19 Identity and Access Management	377
CHAPTER 20 Security Automation and Orchestration	401
CHAPTER 21 Incident Response Activities	409
CHAPTER 22 Data Sources for Supporting Investigations	419

Part 5: Security Program Management and Oversight	425
CHAPTER 23 Effective Security Governance	427
CHAPTER 24 Risk Management	465
CHAPTER 25 Third-Party Risk Assessment and Management	485
CHAPTER 26 Security Compliance	495
CHAPTER 27 Security Audits and Assessments	509
CHAPTER 28 Security Awareness Practices	525
Glossary of Essential Terms	551
Cram Sheet	603
Index	617

Table of Contents

Introduction	xxvi
------------------------	------

Part 1: General Security Concepts **1**

CHAPTER 1:

Security Controls **3**

Nature of Controls	3
Functional Use of Controls	4
Preventive Controls	5
Deterrent Controls	5
Detective Controls	6
Corrective Controls	6
Compensating Controls	6
Directive Controls	7
What Next?	9

CHAPTER 2:

Fundamental Security Concepts **11**

Confidentiality, Integrity, and Availability (CIA)	12
Non-Repudiation	13
Authentication, Authorization, and Accounting (AAA)	13
Gap Analysis	14
Zero Trust	15
Physical Security	18
Bollards	19
Access Control Vestibules	19
Signs, Fencing, and Gates	20
Video Surveillance	20
Security Guards	21
Access Badge	21
Lighting	21
Sensors	22
Deception and Disruption Technology	23
What Next?	26

CHAPTER 3:**Change Management Processes and the Impact to Security 27**

Change Management	28
Business Processes Impacting Security Operations	28
Approval Process	29
Ownership.	29
Stakeholders	29
Impact Analysis	30
Test Results	30
Backout Plan	30
Maintenance Window.	30
Standard Operating Procedure (SOP)	31
Technical Implications.	31
Allow Lists/Deny Lists	32
Restricted Activities	32
Downtime	32
Service Restart.	33
Application Restart.	33
Legacy Applications	34
Dependencies	34
Documentation	35
Version Control	36
What Next?	38

CHAPTER 4:**Cryptographic Solutions 39**

Public Key Infrastructure (PKI)	40
Public and Private Key Usage	41
Key Escrow	42
Encryption	43
Levels and Types	44
Cryptographic Algorithms.	49
Symmetric Algorithms	51
Asymmetric Algorithms.	53
Tools.	55
Trusted Platform Module (TPM)	55
Encryption and Data Obfuscation.	59
Steganography	62
Hashing and Salting	63

Digital Signatures	64
Digital Certificate	67
Certificate Authority (CA)	69
Certificate Revocation	77
OCSP Stapling	78
Pinning	79
What Next?	80

Part 2: Threats, Vulnerabilities, and Mitigations **81**

CHAPTER 5:

Threat Actors and Motivations **83**

Threat Actors	84
Threat Actor Attributes	84
Types of Threat Actors	85
Motivations	90
Data Exfiltration	90
Espionage	91
Service Disruption	91
Blackmail	92
Financial Gain	92
Philosophical/Political Beliefs	92
Ethical	93
Revenge	93
Disruption/Chaos	93
War	94
What Next?	96

CHAPTER 6:

Threat Vectors and Attack Surfaces **97**

Types of Threat Vectors and Attack Surfaces	98
Message-Based	99
Image-Based	101
File-Based	101
Voice Call	102
Removable Device	102
Vulnerable Software	103
Unsupported Systems and Applications	103
Unsecured Networks	104
Open Service Ports	104

Default Credentials	105
Supply Chain	105
Human Vectors/Social Engineering	106
What Next?	114

CHAPTER 7:

Vulnerability Types	115
Application	116
Operating System-Based	118
Web-Based	119
Hardware	120
Virtualization	121
Cloud-Specific	122
Supply Chain	123
Cryptographic	125
Misconfiguration	126
Mobile Device	127
Zero-Day	127
What Next?	130

CHAPTER 8:

Malicious Attacks and Indicators	131
Malware Attacks	132
Ransomware	133
Trojan	133
Worm	134
Spyware	134
Bloatware	135
Virus	136
Keylogger	136
Logic Bomb	136
Rootkit	137
Physical Attacks	138
Brute-Force Attack	138
Radio Frequency Identification (RFID) Cloning Attack	138
Environmental Attack	139
Network Attacks	139
Distributed Denial of Service (DDoS)	140
Domain Name System (DNS) Attacks	142

Wireless	144
On-Path	147
Credential Replay	147
Malicious Code	148
Application Attacks	148
Injection	148
Buffer Overflow	149
Replay	150
Privilege Escalations	150
Forgery	151
Directory Traversal	152
Cryptographic Attacks	153
Downgrade	153
Collision	153
Birthday	154
Password Attacks	154
Indicators of Malicious Activity	156
What Next?	160

CHAPTER 9

Mitigation Techniques for Securing the Enterprise 161

Segmentation	162
Access Control	162
Application Allow List	164
Isolation	165
Patching	165
Encryption	166
Monitoring	167
Least Privilege	167
Configuration Enforcement	167
Decommissioning	168
Hardening Techniques	168
Encryption	168
Installation of Endpoint Protection	169
Host-based Firewall	170
Host-based Intrusion Prevention System (HIPS)	170
Disabling Ports/Protocols	171
Default Password Changes	173
Removal of Unnecessary Software	173
What Next?	176

Part 3: Security Architecture 177

**CHAPTER 10:
Security Implications of Architecture Models 179**

- Architecture and Infrastructure Concepts 180
 - Cloud 180
 - Infrastructure as Code (IaC) 186
 - Serverless 187
 - Microservices 188
 - Network Infrastructure 189
 - On-Premises 192
 - Centralized vs. Decentralized 192
 - Containerization 193
 - Virtualization 195
 - IoT 197
 - Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) 198
 - Real-Time Operating System (RTOS) 200
 - Embedded Systems 200
 - High Availability 201
- Considerations 201
 - Availability 202
 - Resilience 202
 - Cost 203
 - Responsiveness 203
 - Scalability 204
 - Ease of Deployment 204
 - Risk Transference 205
 - Ease of Recovery 205
 - Patch Availability 205
 - Inability to Patch 206
 - Power 206
 - Compute 207
- What Next? 209

**CHAPTER 11:
Enterprise Architecture Security Principles 211**

- Infrastructure Considerations 212
 - Device Placement 212
 - Security Zones 213

Attack Surface	214
Connectivity	214
Failure Modes	214
Device Attribute	215
Network Appliances	216
Port Security	220
Firewall Types	222
Secure Communication/Access	224
Virtual Private Network (VPN)	225
Remote Access	225
Tunneling	226
Software-Defined Wide Area Network (SD-WAN)	227
Secure Access Service Edge (SASE)	228
Selection of Effective Controls	228
What Next?	232

CHAPTER 12:

Data Protection Strategies 233

Data Types	234
Regulated	234
Trade Secret	235
Intellectual Property	235
Legal Information	236
Financial Information	236
Human- and Non-Human-Readable	236
Data Classifications	237
General Data Considerations	238
Data States	239
Data Sovereignty	239
Geolocation	240
Methods to Secure Data	240
Geographic Restrictions	240
Encryption	241
Hashing	241
Masking	242
Tokenization	242
Obfuscation	242
Segmentation	243
Permission Restrictions	243
What Next?	246

CHAPTER 13:
Resilience and Recovery in Security Architecture 247

- High Availability 248
- Site Considerations 249
- Platform Diversity 251
- Multicloud Systems 252
- Continuity of Operations 252
- Capacity Planning 253
- Testing 254
- Backups 255
 - Onsite/Offsite 257
 - Frequency 258
 - Encryption 258
 - Snapshots 259
 - Recovery 260
 - Replication 260
 - Journaling 261
- Power 261
- What Next? 264

Part 4: Security Operations 265

CHAPTER 14:
Securing Resources 267

- Secure Baselines 268
- Hardening Targets 270
 - Mobile Devices 270
 - Workstations 271
 - Switches 272
 - Routers 273
 - Cloud Infrastructure 273
 - Servers 274
 - ICS/SCADA 275
 - Embedded Systems 276
 - RTOS 277
 - IoT Devices 277
- Wireless Devices 278
- Mobile Solutions 281
 - Mobile Device Management (MDM) 282

Deployment Models	282
Connection Methods	283
Wireless Security Settings	285
Wi-Fi Protected Access Version 3 (WPA3).	285
AAA/Remote Authentication Dial-In User Service (RADIUS)	286
Cryptographic Protocols	287
Authentication Protocols	288
Application Security	289
Sandboxing	290
Monitoring	291
What Next?	293
CHAPTER 15:	
Hardware, Software, and Data Asset Management	295
Acquisition/Procurement Process	296
Assignment/Accounting	297
Ownership	297
Classification	297
Monitoring and Asset Tracking	299
Inventory	300
Enumeration	300
Disposal/Decommissioning	300
Sanitization	301
Destruction	302
Certification	302
Data Retention	303
What Next?	305
CHAPTER 16:	
Vulnerability Management	307
Identification Methods	308
Vulnerability Scan	308
Application Security	309
Threat Feeds	311
Penetration Testing	314
Responsible Disclosure Program	316
System/Process Audit	316
Analysis	316

- Confirmation 317
- Prioritization 317
- Common Vulnerability Scoring System (CVSS) 318
- Common Vulnerability Enumeration (CVE) 319
- Vulnerability Classification 320
- Exposure Factor 321
- Environmental Variables 321
- Industry/Organizational Impact 321
- Risk Tolerance 322
- Vulnerability Response and Remediation 322
 - Patching 322
 - Insurance 323
 - Segmentation 324
 - Compensating Controls 324
 - Exceptions and Exemptions 324
- Validation of Remediation 325
 - Rescanning 325
 - Audit 326
 - Verification 326
- Reporting 326
- What Next? 328

CHAPTER 17:

Security Alerting and Monitoring 329

- Monitoring Computing Resources 330
 - Systems 330
 - Applications 330
 - Infrastructure 331
- Activities 332
 - Log Aggregation 332
 - Alerting 333
 - Scanning 334
 - Reporting 334
 - Archiving 334
 - Alert Response and Remediation/Validation 335
- Tools 336
 - Security Content Automation Protocol (SCAP) 336
 - Benchmarks 337
 - Agents/Agentless 337

Security Information and Event Management (SIEM)	338
Antivirus	341
Data Loss Prevention (DLP)	341
Simple Network Management Protocol (SNMP) Traps	342
NetFlow	343
Vulnerability Scanners	344
What Next?	347

CHAPTER 18:

Enterprise Security Capabilities	349
Firewall	350
Rules	350
Access Lists	352
Ports/Protocols	353
Screened Subnet	353
IDS/IPS	354
Trends	355
Signatures	356
Web Filter	357
Agent-Based	358
Centralized Proxy	359
Universal Resource Locator (URL) Scanning	360
Content Categorization	360
Block Rules	360
Reputation	361
Operating System Security	361
Group Policy	362
SELinux	363
Implementation of Secure Protocols	363
Protocol Selection	363
Port Selection	365
Transport Method	365
DNS Filtering	366
Email Security	367
DMARC, DKIM, SPF, and Gateway	368
File Integrity Monitoring	369
Data Loss Prevention (DLP)	370
Network Access Control (NAC)	371

Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR)	372
User Behavior Analytics	373
What Next?	375

CHAPTER 19:

Identity and Access Management	377
Provisioning/De-provisioning User Accounts	378
Permission Assignments and Implications	379
Identity Proofing	381
Federation and Single Sign-On (SSO)	382
Interoperability	385
Attestation	385
Access Controls	386
Multifactor Authentication (MFA)	388
Implementations	389
Factors	394
Password Concepts	395
Password Managers	397
Passwordless	397
Privileged Access Management Tools	397
What Next?	400

CHAPTER 20:

Security Automation and Orchestration	401
Use Cases of Automation and Scripting	402
User and Resource Provisioning	402
Guard Rails	403
Security Groups	403
Ticket Creation and Escalation	403
Enabling/Disabling Services and Access	404
Continuous Integration and Testing	404
Integrations and Application Programming Interfaces (APIs)	405
Benefits	405
Other Considerations	406
What Next?	408

CHAPTER 21:	
Incident Response Activities	409
Incident Response Process	410
Training and Testing	411
Root Cause Analysis (RCA)	412
Threat Hunting	413
Digital Forensics	414
What Next?	417
CHAPTER 22:	
Data Sources for Supporting Investigations	419
Log Data	419
Data Sources	421
What Next?	423
Part 5: Security Program Management and Oversight	425
CHAPTER 23:	
Effective Security Governance	427
Governing Framework	428
Types of Governance Structures	430
Monitoring and Revision	432
Policies	433
Acceptable Use Policy (AUP)	433
Information Security Policy	435
Business Continuity Policies	437
Disaster Recovery Policies	438
Incident Response Policy	440
Software Development Lifecycle Policy	441
Change Management Policy	443
Standards	445
Procedures	447
Guidelines	452
External Considerations	453
Regulatory and Nonregulatory Requirements	455
Industry-Specific Frameworks	458
Roles and Responsibilities for Systems and Data	460
What Next?	464

CHAPTER 24:

Risk Management 465

- Risk Identification 466
- Risk Assessment 466
- Risk Analysis 468
 - Qualitative Risk Analysis 469
 - Quantitative Risk Analysis 470
 - Single Loss Expectancy 471
 - Annual Rate of Occurrence 471
 - Annual Loss Expectancy 472
- Risk Register 472
- Risk Appetite and Tolerance 474
- Risk Management Strategies 475
- Risk Reporting 477
- Business Impact Analysis 478
 - RTO and RPO 479
 - MTTE, MTBF, and MTTR 479
- What Next? 483

CHAPTER 25:

Third-Party Risk Assessment and Management 485

- Third-Party Risk Management 486
 - Vendor Assessment 486
 - Vendor Selection 488
 - Agreement Types 489
 - Vendor Monitoring 491
 - Rules of Engagement 492
- What Next? 494

CHAPTER 26:

Security Compliance 495

- Compliance Reporting and Monitoring 496
 - Compliance Reporting 496
 - Consequences of Non-Compliance 497
 - Compliance Monitoring 499
- Privacy 501
 - Privacy Data Roles 501
 - Data Inventory and Retention 503

<i>Legal Implication of Data Privacy</i>	504
Right to Be Forgotten	505
What Next?	507
CHAPTER 27:	
Security Audits and Assessments	509
Audits and Assessments	510
Attestation	510
Internal Audits and Assessments	511
External Audits and Assessments	512
Penetration Testing	513
Active and Passive Reconnaissance	516
Physical Tests	517
Offensive, Defensive, and Integrated	518
Penetration Test Environments	520
What Next?	523
CHAPTER 28:	
Security Awareness Practices	525
Security Awareness	526
Phishing Campaigns	526
Anomalous Behavior Recognition	532
User Guidance and Training	533
Reporting and Monitoring	542
Development and Execution	545
What Next?	550
Glossary of Essential Terms	551
Cram Sheet	603
Index	617

About the Authors

Robert Shimonski, CASP+, CySA+, PenTest+, Security+, is a technology executive specializing in healthcare IT for one of the largest health systems in America. In his current role, Rob is responsible for bringing operational support and incident response into the future with the help of new technologies such as cloud and artificial intelligence. His current focus is on deploying securely to the cloud (Azure, AWS, and Google), DevOps, DevSecOps, and AIOps. Rob spent many years in the technology “trenches,” handling networking and security architecture, design, engineering, testing, and development efforts for global projects. A go-to person for all things security related, Rob has been a major force in deploying security-related systems for 25+ years. Rob also worked for various companies reviewing and developing security curriculum as well as other security-related books, technical articles, and publications based on technology deployment, testing, hacking, pen testing, and many other aspects of security. Rob holds dozens of technology certifications, including 20+ CompTIA certifications, SANS.org GIAC, GSEC, and GCIH, as well as many vendor-based cloud-specialized certifications from Google, Microsoft Azure, and Amazon AWS. Rob is considered a leading expert in prepping others to achieve certification success.

Marty M. Weiss has spent his career serving in the U.S. Navy and as a civilian helping large organizations with their information security. He has a Bachelor of Science degree in computer studies from the University of Maryland Global Campus and an MBA from the Isenberg School of Management at the University of Massachusetts Amherst. He also holds several certifications, including CISSP, CISA, and Security+. Having authored numerous acclaimed books on information technology and security, he is now diving into his next endeavor—a seductive romance novel where love and cybersecurity collide in a high-stakes adventure.

Dedications

This book is dedicated to my dad, who passed during the writing of this book. Thank you for being a great dad. You will always be remembered and missed.
—Robert Shimonski

Dedicated to those who embrace both privacy and vulnerability in their pursuit of security.
—Marty Weiss

Acknowledgments

Robert Shimonski: Thank you to the entire team that made this book a reality. Countless people were involved, including Carole Jelen, Nancy Davis, Ellie Bru, Chris Crayton, Mandie Frank, Bart Reed, and Raymond Lacoste. Without your help, this book would never be as good as it is! Also, to my co-author Marty, thanks for being a great teammate. I would also like to thank you, the reader, for showing interest in not only growing through learning but for trusting our brand. Thank you!

Marty Weiss: Thank you Carole, Nancy, Ellie, Mandie, Robert, Raymond, Chris, Bart, and the entire team that helped to bring this book together. Big thanks to everyone special and close to me—mom, dad, siblings, 5 a.m. dream team, Kelly, Kobe, Max, Ollie, and Anabelle. Finally, thank you Elliott for reminding us that they should not control the digital ledger.

About the Technical Reviewers

Raymond Lacoste has dedicated his career to developing the skills of those interested in IT. In 2001, he began to mentor hundreds of IT professionals pursuing their Cisco certification dreams. This role led to teaching Cisco courses full time. Raymond is currently a master instructor for Cisco Enterprise Routing and Switching, AWS, ITIL, and Cybersecurity at StormWind Studios. Raymond treats all technologies as an escape room, working to uncover every mystery in the protocols he works with. Along this journey, Raymond has passed more than 120 exams, and his office wall includes certificates from Microsoft, Cisco, ISC2, ITIL, AWS, and CompTIA. If you were visualizing Raymond's office, you'd probably expect the usual network equipment, certifications, and awards. Those certainly take up space, but they aren't his pride and joy. Most impressive, at least to Raymond, is his gemstone and mineral collection; once he starts talking about it, he just can't stop. Who doesn't get excited by a wondrous barite specimen in a pyrite matrix? Raymond presently resides with his wife and two children in eastern Canada, where they experience many adventures together.

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge.

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: community@informit.com

Reader Services

Register your copy of *CompTIA Security+ SY0-701 Exam Cram* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780138225575 and click **Submit**. When the process is complete, you will find any available bonus content under Registered Products.

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

Introduction

Welcome to *CompTIA Security+ SY0-701 Exam Cram*. This book helps you get ready to take and pass the CompTIA Security+ SY0-701 exam.

This book is designed to remind you of everything you need to know to pass the SY0-701 certification exam. Each chapter includes a number of practice questions that should give you a reasonably accurate assessment of your knowledge, and, yes, we've provided the answers and their explanations for these questions. Read this book, understand the material, and you'll stand a very good chance of passing the real test.

Exam Cram books help you understand the subjects and materials you need to know to pass CompTIA certification exams. *Exam Cram* books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, the authors streamline and highlight the pertinent information by presenting and dissecting the questions and problems they've discovered that you're likely to encounter on a CompTIA test.

We strongly recommend that you spend some time installing and working with security tools and experimenting with the many network and security-related resources provided with the various operating systems. The Security+ exam focuses on such activities and the knowledge and skills they can provide you. Nothing beats hands-on experience and familiarity when it comes to understanding the questions you're likely to encounter on a certification test. Book learning is essential, but without a doubt, hands-on experience is the best teacher of all!

Let's begin by looking at preparation for the exam.

How to Prepare for the Exam

This text follows the official exam objectives closely to help ensure your success. The CompTIA exam covers five domains and 28 objectives. This book is divided into five parts and 28 chapters, aligning with those domains and objectives. The official objectives from CompTIA can be found at <https://www.comptia.org/training/resources/exam-objectives>.

As you examine the numerous exam topics now covered in Security+, resist the urge to panic! This book you are reading will provide you with the knowledge

(and confidence) you need to succeed. You just need to make sure you read it and follow the guidance it provides throughout your Security+ journey.

Practice Tests

This book is filled with practice exam questions to get you ready! Cram quizzes end each chapter, and each question also includes a complete explanation.

In addition, the book includes two additional full practice tests in the Pearson Test Prep software, available to you either online or as an offline Windows application. To access the practice exams developed with this book, see the instructions in the “Pearson Test Prep Practice Test Software” section.

In case you are interested in more practice exams than are provided with this book, Pearson IT Certification publishes a Premium Edition eBook and Practice Test product. In addition to providing you with two eBook files (EPUB and PDF), this product provides you with two additional exams’ worth of questions. The Premium Edition version also offers you a link to the specific section in the book that presents an overview of the topic covered in the question, allowing you to easily refresh your knowledge. Learn more at www.pearsonitcertification.com.

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. You can take this exam either virtually at home or at a testing center. Make sure you select the option that best suits you. At the time of writing, the cost to take the Security+ exam is US\$404 for individuals. Students in the United States are eligible for a significant discount. In addition, check with your employer, as many workplaces provide reimbursement programs for certification exams. For more information about these discounts, you can contact a local CompTIA sales representative, who can answer any questions you might have. If you don’t pass, you can take the exam again for the same cost as the first attempt until you pass. The test is administered by Pearson VUE testing centers, with locations globally. In addition, the CompTIA Security+ certification is a requirement for many within the U.S. military, and testing centers are available on some military bases.

You will have 90 minutes to complete the exam. The exam consists of a maximum of 90 questions. If you have prepared, you should find that this is plenty of time to properly pace yourself and review the exam before submission.

Arriving at the Exam Location

If you do select to take the exam at an exam location, here is what you should know: As with any other examination, arrive at the testing center early (at least 15 minutes). Be prepared! You need to bring two forms of identification (one with a picture). The testing center staff requires proof that you are who you say you are and that someone else is not taking the test for you. Arrive early, because if you are late, you will be barred from entry and will not receive a refund for the cost of the exam.

ExamAlert

You'll be spending a lot of time in the exam room. Plan on using the full 90 minutes allotted for your exam and surveys. Policies differ from location to location regarding bathroom breaks, so check with the testing center before beginning the exam.

In the Testing Center

You will not be allowed to take into the examination room study materials or anything else that could raise suspicion that you're cheating. This includes practice test material, books, exam prep guides, and other test aids. The testing center will provide you with scratch paper and a pen or pencil. These days, this often comes in the form of an erasable whiteboard.

Examination results are available immediately after you finish the exam. After submitting the exam, you will be notified as to whether you have passed or failed. We trust that if you are reading this book, you will pass. The test administrator will also provide you with a printout of your results.

About This Book

The ideal reader for an *Exam Cram* book is someone seeking certification. However, it should be noted that an *Exam Cram* book is a very easily readable, rapid presentation of facts. Therefore, an *Exam Cram* book is also extremely useful as a quick reference manual.

The book is designed so that you can either read it cover to cover or jump across chapters, as needed. Because the book chapters align with the exam objectives, some chapters may have slight overlap on topics. Where required, references to the other chapters are provided for you. If you need to brush up on a topic or if you have to bone up for a second try at the exam, you can use the index, table of contents, or Table I.1 to go straight to the topics and questions you need to study. Beyond helping you prepare for the test, we think you'll find this book useful as a tightly focused reference on some of the most important aspects of the Security+ certification.

This book includes other helpful elements in addition to the actual logical, step-by-step learning progression of the chapters. *Exam Cram* books use elements such as ExamAlerts, notes, and practice questions to make information easier to read and absorb. This text also includes a Glossary to assist you.

Note

Reading this book from start to finish is not necessary; it is set up so that you can quickly jump back and forth to find sections you need to study.

Use the *Cram Sheet* to remember last-minute facts immediately before the exam. Use the practice questions to test your knowledge. You can always brush up on specific topics in detail by referring to the table of contents and the index. Even after you achieve certification, you can use this book as a rapid-access reference manual.

Exam Objectives

Table I.1 lists the skills the SY0-701 exam measures and the chapter in which each objective is discussed.

TABLE I.1 **CompTIA Security+ SY0-701 Exam Domains and Objectives**

Exam Domain	Objective	Chapter in Book that Covers It
1.0 General Security Concepts	1.1 Compare and contrast various types of security controls.	Chapter 1
1.0 General Security Concepts	1.2 Summarize fundamental security concepts.	Chapter 2
1.0 General Security Concepts	1.3 Explain the importance of change management processes and the impact to security.	Chapter 3
1.0 General Security Concepts	1.4 Explain the importance of using appropriate cryptographic solutions.	Chapter 4
2.0 Threats, Vulnerabilities, and Mitigations	2.1 Compare and contrast common threat actors and motivations.	Chapter 5
2.0 Threats, Vulnerabilities, and Mitigations	2.2 Explain common threat vectors and attack surfaces.	Chapter 6
2.0 Threats, Vulnerabilities, and Mitigations	2.3 Explain various types of vulnerabilities.	Chapter 7
2.0 Threats, Vulnerabilities, and Mitigations	2.4 Given a scenario, analyze indicators of malicious activity.	Chapter 8
2.0 Threats, Vulnerabilities, and Mitigations	2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	Chapter 9
3.0 Security Architecture	3.1 Compare and contrast security implications of different architecture models.	Chapter 10
3.0 Security Architecture	3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	Chapter 11
3.0 Security Architecture	3.3 Compare and contrast concepts and strategies to protect data.	Chapter 12
3.0 Security Architecture	3.4 Explain the importance of resilience and recovery in security architecture.	Chapter 13
4.0 Security Operations	4.1 Given a scenario, apply common security techniques to computing resources.	Chapter 14
4.0 Security Operations	4.2 Explain the security implications of proper hardware, software, and data asset management.	Chapter 15
4.0 Security Operations	4.3 Explain various activities associated with vulnerability management.	Chapter 16

Exam Domain	Objective	Chapter in Book that Covers It
4.0 Security Operations	4.4 Explain security alerting and monitoring concepts and tools.	Chapter 17
4.0 Security Operations	4.5 Given a scenario, modify enterprise capabilities to enhance security.	Chapter 18
4.0 Security Operations	4.6 Given a scenario, implement and maintain identity and access management.	Chapter 19
4.0 Security Operations	4.7 Explain the importance of automation and orchestration related to secure operations.	Chapter 20
4.0 Security Operations	4.8 Explain appropriate incident response activities.	Chapter 21
4.0 Security Operations	4.9 Given a scenario, use data sources to support an investigation.	Chapter 22
5.0 Security Program Management and Oversight	5.1 Summarize elements of effective security governance.	Chapter 23
5.0 Security Program Management and Oversight	5.2 Explain elements of the risk management process.	Chapter 24
5.0 Security Program Management and Oversight	5.3 Explain the processes associated with third-party risk assessment and management.	Chapter 25
5.0 Security Program Management and Oversight	5.4 Summarize elements of effective security compliance.	Chapter 26
5.0 Security Program Management and Oversight	5.5 Explain types and purposes of audits and assessments.	Chapter 27
5.0 Security Program Management and Oversight	5.6 Given a scenario, implement security awareness practices.	Chapter 28

The Chapter Elements

Each *Exam Cram* book has chapters that follow a predefined structure. This structure makes *Exam Cram* books easy to read and provides a familiar format for all *Exam Cram* books. The following elements typically are used:

- ▶ Chapter topics
- ▶ Essential Terms and Components
- ▶ Cram Quizzes

- ▶ ExamAlerts
- ▶ Notes
- ▶ Available exam preparation software practice questions and answers

Note

Bulleted lists, numbered lists, tables, and graphics are also used where appropriate. A picture can paint a thousand words sometimes, and tables can help to associate different elements with each other visually.

Now let's look at each of the elements in detail:

- ▶ **Chapter topics:** Each chapter contains details of all subject matter listed in the table of contents for that particular chapter. The objective of an *Exam Cram* book is to cover all the important facts without giving too much detail. When examples are required, they are included.
- ▶ **Essential Terms and Components:** The start of every chapter contains a list of terms and concepts you should understand. These are all defined in the book's accompanying Glossary.
- ▶ **Cram Quizzes:** Each chapter concludes with multiple-choice questions to help ensure you have gained familiarity with the chapter content.
- ▶ **ExamAlerts:** ExamAlerts address exam-specific, exam-related information. An ExamAlert addresses content that is particularly important, tricky, or likely to appear on the exam. An ExamAlert looks like this:

ExamAlert

Make sure you remember the different ways in which you can access a router remotely. Know which methods are secure and which are not.

- ▶ **Notes:** Notes typically contain useful information that is not directly related to the topic currently under consideration. To avoid breaking up the flow of the text, they are set off from the regular text.

Note

This is a note.

Other Book Elements

Most of this *Exam Cram* book on Security+ follows the consistent chapter structure already described. However, there are various important elements that are not part of the standard chapter format. These elements apply to the entire book as a whole.

- ▶ **Practice questions:** Exam-preparation questions conclude each chapter.
- ▶ **Answers and explanations for practice questions:** These follow each practice question, providing answers and explanations to the questions.
- ▶ **Glossary:** The Glossary defines important terms used in this book.
- ▶ **Cram Sheet:** The Cram Sheet is a quick-reference guide to important facts and is useful for last-minute preparation. The Cram Sheet provides a simple summary of the facts that may be most difficult to remember.
- ▶ **Companion website:** The companion website for your book allows you to access several digital assets that come with your book, including the following:
 - ▶ Pearson Test Prep software (both online and Windows desktop versions)
 - ▶ Key Terms Flash Cards application
 - ▶ A PDF version of the Cram Sheet

To access the book's companion website, simply follow these steps:

1. Register your book by going to **PearsonITCertification.com/register** and entering the ISBN **9780138225575**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, see the following instructions.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- ▶ You can get your access code by registering the print ISBN (9780138225575) on pearsonitcertification.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the **Registered Products** tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.
- ▶ If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonitcertification.com, click **Account** to see details of your account, and click the **Digital Purchases** tab.

Note

After you register your book, your code can always be found in your account on the Registered Products tab.

Once you have the access code, to find instructions about both the Pearson Test Prep web app and the desktop app, follow these steps:

Step 1: Open this book's companion website, as shown earlier in this Introduction, under the heading, "Other Book Elements."

Step 2: Click the Practice Test Software button.

Step 3: Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsonstestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

In the exam settings screen, you can choose to take exams in one of three modes:

- ▶ Study Mode
- ▶ Practice Exam Mode
- ▶ Flash Card Mode

Study Mode allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options, as it presents a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

In addition to these three modes, you can select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with an exam of targeted questions that cover topics in every chapter. The Cram Quizzes printed in the book are available to you and two additional exams of unique questions. You can have the test engine serve up exams from all banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time you are allowed for taking the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. You must be connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate an exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the **Tools** tab and click the **Update Application** button. This will ensure you are running the latest version of the software engine.

Contacting the Authors

Hopefully, this book provides you with the tools you need to pass the Security+ SY0-701 exam. Feedback is appreciated. You can follow and contact the authors on X (formerly known as Twitter) @martyweiss and @robshimonski.

Thank you for selecting our book; we have worked to apply the same concepts in this book that we have used in the hundreds of training classes we have taught. Spend your study time wisely and you, too, can achieve the Security+ designation. Good luck on the exam, although if you carefully work through this text, you will certainly minimize the amount of luck required!

Figure Credits

Figure 8.1: WannaCry

Figure 18.4: WatchGuard Technologies, Inc.

Figure 18.1, 18.2, 18.5-18.7, 19.1: Microsoft Corporation

Figure 19.2: Apple, Inc

CHAPTER 24

Risk Management

This chapter covers the following official Security+ exam objective:

- ▶ 5.2 Explain elements of the risk management process.

Essential Terms and Components

- ▶ Risk identification
- ▶ Risk assessment
- ▶ Ad hoc
- ▶ Recurring
- ▶ One-time
- ▶ Continuous
- ▶ Risk analysis
- ▶ Qualitative
- ▶ Quantitative
- ▶ Single loss expectancy (SLE)
- ▶ Annualized loss expectancy (ALE)
- ▶ Annualized rate of occurrence (ARO)
- ▶ Risk register
- ▶ Key risk indicators
- ▶ Risk owners
- ▶ Risk thresholds
- ▶ Risk tolerance
- ▶ Risk appetite
- ▶ Expansionary
- ▶ Conservative
- ▶ Neutral
- ▶ Risk management strategies
- ▶ Risk reporting
- ▶ Business impact analysis
- ▶ Recovery time objective (RTO)

- ▶ Recovery point objective (RPO)
- ▶ Mean time to repair (MTTR)
- ▶ Mean time to between failures (MTBF)

Risk Identification

Risk identification is the initial step in the risk management process, aimed at identifying potential threats and vulnerabilities that could adversely affect an organization. This ensures that the organization can proactively address risks through planning and implementation of security measures.

A threat can be thought of as the potential that a vulnerability will be identified and exploited. Analyzing threats can help an organization develop security policies and prioritize securing resources. Threat assessments are performed to determine the best approaches to securing the environment against a threat or class of threats. Threats might exist, but if an environment has no vulnerabilities, it faces little or no risk. Likewise, little or no risk affects environments that have vulnerability without threat. Consider the simple analogy of a hurricane. Few would argue that a hurricane represents a threat. However, consider a home on the coast in Florida and a home inland in the Midwest. The former is certainly vulnerable to a hurricane, whereas the latter is not.

Probability is the likelihood that an event will occur. In assessing risk, it is important to estimate the probability or likelihood that a threat will occur. Assessing the likelihood of occurrence of some types of threats is easier than assessing other types. For example, you can use frequency data to estimate the probability of natural disasters. You might also be able to use the mean time to failure (MTTF) and mean time to repair (MTTR), both covered later in this chapter, to estimate the probability of component problems. Determining the probability of attacks by human threat sources is difficult. Threat source likelihood is assessed using skill level, motive, opportunity, and size. Vulnerability likelihood is assessed using ease of discovery, ease of exploit, awareness, and intrusion detection.

Risk Assessment

Risk assessment is the process of analyzing identified risks to evaluate the likelihood of their occurrence and their potential impact. This evaluation is required for prioritizing risks and formulating strategies to mitigate them effectively.

Risk is the possibility of, or exposure to, loss or danger from a threat. Risk management is the process of identifying and reducing risk to a level that is acceptable and then implementing controls to maintain that level. Risk comes in various types. Risk can be internal, external, or multiparty. Banks provide a great example of multiparty risk: Because of the ripple effects, issues at banks have effects on other banks and financial systems.

To determine the relative danger of an individual threat or to measure the relative value across multiple threats to better allocate resources designated for risk mitigation, it is necessary to map the resources, identify threats to each, and establish a metric for comparison. A business impact analysis (BIA) helps identify services and technology assets as well as provides a process by which the relative value of each identified asset can be determined if it fails one or more of the CIA (confidentiality, integrity, and availability) requirements. The failure to meet one or more of the CIA requirements is often a sliding scale, with increased severity as time passes. Recovery point objectives (RPOs) and recovery time objectives (RTOs) in incident handling, business continuity, and disaster recovery must be considered when calculating risk. BIA, RPOs, and RTOs are covered further later in this chapter.

Risk assessments should rarely if ever be a one-time event for an organization. The frequency with which these are conducted, however, can vary depending on various factors regarding the organization's risk landscape, regulatory requirements, and level of change across their environments. For example, a small, stable private organization may find an annual risk assessment sufficient. On the other hand, a large, dynamic organization operating across high-risk environments, where emerging risks may pose challenges, should opt for more frequent assessments. Generally, risk assessments are conducted adopting the following frequencies:

- ▶ Ad hoc
- ▶ One-time
- ▶ Recurring
- ▶ Continuous

Ad hoc risk assessments are conducted in response to specific incidents or triggers. For example, if a company encounters a significant security breach, it would conduct an ad hoc risk assessment to understand the scope and severity of the risk posed by the breach. Ad hoc assessments can also be made if a new business opportunity arises, and the company needs to carry out an immediate assessment of the associated risks.

One-time risk assessments are often conducted for specific events or changes. For instance, when introducing a new system, launching a new product, or

during a business merger or acquisition, a company would conduct a one-time assessment to understand the potential risks associated with these activities. A one-time assessment helps organizations anticipate and mitigate risks associated with the change.

Recurring assessments are conducted at regular intervals, such as annually, semi-annually, or quarterly, depending on the organization's requirements and nature of the industry. Recurring risk assessments allow organizations to stay on top of any changes to their risk profile. The frequency depends on the level of risk an organization faces and the rate of change in its external environment, as well as internal factors such as a change in business strategy.

In a **continuous** risk assessment approach, the risk environment is monitored in real time, and risks are assessed on an ongoing basis. This approach relies on established **key risk indicators (KRIs)** to evaluate the company's risk profile. When thresholds are breached, risk assessments are triggered. As with other approaches, a continuous risk assessment approach requires balancing risk visibility against resource commitment, but it may provide the most complete and timely understanding of risk in more volatile environments.

Risk Analysis

Risk analysis helps align security objectives with business objectives. It is a process that deals with the calculation of risk and the return on investment for security measures. By identifying risks, estimating the effects of potential threats, and identifying ways to mitigate these risks in a cost effective manner, organizations can ensure that the cost of prevention does not outweigh the benefits.

The risk analysis process involves several key steps to assess and manage risk effectively:

1. **Identify threats:** Recognize potential threats that could exploit vulnerabilities.
2. **Identify vulnerabilities:** Determine weaknesses within the system that could be exploited by threats.
3. **Determine the likelihood of occurrence:** Evaluate how probable it is for a threat to occur and exploit a vulnerability.
4. **Determine the magnitude of impact:** Assess the potential severity of the damage or loss if a threat materializes.
5. **Determine the risk:** Calculate the level of risk using the simple equation $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$.

This process helps in understanding the complex relationship between threats, vulnerabilities, and their potential impacts, emphasizing the importance of assessing the likelihood that a threat will actually occur.

After identifying and assessing risks, it's important that you categorize and prioritize them based on their likelihood of occurrence and potential impact. This prioritization helps in formulating appropriate response strategies:

- ▶ High-level threats may necessitate immediate corrective measures.
- ▶ Medium-level threats might require developing an action plan for reasonable implementation.
- ▶ Low-level threats could be dealt with as feasible or might be accepted as part of the organization's risk threshold.

The assessment of impact alongside risk likelihood is needed to understand the potential consequences of risk events.

ExamAlert

Risk is the product of threat, vulnerability, and impact.

Qualitative Risk Analysis

Qualitative risk analysis is a subjective approach that assesses risks based on non-numeric criteria. It involves using techniques such as brainstorming, focus groups, and surveys to gauge the significance of different risks and their impact. This method allows for a relative projection of risk for each threat, using a risk matrix or heat map to visualize the probability (from very low to very high) and impact (from very low to very high) of potential risks.

To facilitate this assessment, Table 24.1 provides a risk matrix that can help you understand the level of risk as either low, medium, or high for both likelihood and impact. The table organizes risk levels based on a combination of likelihood scores, ranging from very low to very high, and levels of impact, ranging from very low to very high, resulting in the assignment of an overall risk level.

TABLE 24.1 **Level of Risk Based on Likelihood and Impact**

Likelihood	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Medium	High	High	High	High
High	Low	Medium	High	High	High

Likelihood	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Moderate	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	Medium

The preceding matrix underscores the principle that risk is not just about the potential for a threat to occur but also about the significance of its impact. By categorizing risks into these levels, organizations can prioritize their risk management efforts more effectively, focusing on mitigating the most important risks first.

Despite its subjective nature, and the need for expert judgment, qualitative analysis provides essential insights into risk prioritization, especially when quantitative data is unavailable.

Quantitative Risk Analysis

Quantitative risk analysis offers an objective means to evaluate risk, assigning numerical values to the potential loss and the likelihood of risk occurrence. This method calculates the degree of risk based on the estimation of potential losses and the quantification of unwanted events, utilizing concepts such as **single loss expectancy (SLE)**, **annual rate of occurrence (ARO)**, and **annual loss expectancy (ALE)**.

Quantitative analysis provides clear measures of relative risk and expected return on investment, making it easier for senior management to comprehend and make informed decisions. However, it requires significant effort and time to collect and analyze all related data, making it more labor-intensive than qualitative analysis. Furthermore, qualitative measures tend to be less precise, more subjective, and more difficult in assigning direct costs for measuring return on investment (ROI) and rate of return on investment (RROI).

Because a quantitative assessment is less subjective than a qualitative one, the process requires that a value be assigned to each of the various components. To perform a quantitative risk assessment, an estimation of potential losses is calculated. Next, the likelihood of some unwanted event is quantified, based on the threat analysis. Finally, depending on the potential loss and likelihood, the quantitative process arrives at the degree of risk. Each step relies on the concepts of single loss expectancy, annual rate of occurrence, and annual loss expectancy.

ExamAlert

Remember the difference between quantitative (numeric) and qualitative (subjective/relative) measures. Quantitative (think “quantity”) measures are expressed numerically, whereas qualitative (think “quality”) measures are expressed as “good” or “bad.”

Single Loss Expectancy

Single loss expectancy (SLE) is the expected monetary loss every time a risk occurs. SLE equals asset value multiplied by the threat *exposure factor*, which is the percentage of the asset lost in a successful attack. The formula looks like this:

$$\text{Asset Value} \times \text{Exposure Factor} = \text{SLE}$$

Consider an example of SLE using denial-of-service (DoS) attacks. Firewall logs indicate that the organization was hit hard one time per month by DoS attacks in each of the past 6 months. You can use this historical data to estimate that you likely will be hit 12 times per year. This information helps you calculate the SLE and the ALE. (The ALE is explained in greater detail shortly.)

An asset is any resource that has value and must be protected. Determining an asset’s value can most mean determining the cost to replace the asset if it is lost. Simple property examples fit well here, but figuring asset value is not always so straightforward. Other considerations could be necessary, including the value of the asset to adversaries, the value of the asset to the organization’s mission, and the liability issues that would arise if the asset were compromised.

The exposure factor is the percentage of loss that a realized threat could have on a certain asset. In the DoS example, imagine that 25% of business would be lost if a DoS attack succeeded. The daily sales from the website are \$100,000, so the SLE would be \$25,000 ($\text{SLE} = \$100,000 \times 0.25$). The possibility of certain threats is greater than that of others. Historical data presents the best method of estimating these possibilities.

Annual Rate of Occurrence

The **annual rate of occurrence (ARO)** is the estimated possibility of a specific threat taking place in a 1-year time frame. The possible range of frequency values is from 0.0 (the threat is not expected to occur) to some number whose magnitude depends on the type and population of threat sources. When the probability that a DoS attack will occur is 50%, the ARO is 0.5. After you

calculate the SLE, you can calculate the ALE, which gives you the probability of an event happening over a single year.

Annual Loss Expectancy

The **annual loss expectancy (ALE)** is the monetary loss that can be expected for an asset from risk over a 1-year period. ALE equals SLE times ARO:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

ALE can be used directly in a cost/benefit analysis. Going back to our earlier example, if the SLE is estimated at \$25,000 and the ARO is 0.5, the ALE is \$12,500 ($\$25,000 \times 0.5 = \$12,500$). In this case, spending more than \$12,500 to mitigate risk might not be prudent because the cost would outweigh the risk.

ExamAlert

Remember the following for the exam:

- ▶ SLE is the expected monetary loss every time a risk occurs, and it equals Asset Value \times Exposure Factor.
- ▶ ARO is a numeric representation of the estimated possibility of a specific threat taking place in a 1-year time frame.
- ▶ ALE is the monetary loss that can be expected for an asset from risk over a 1-year period, and it equals SLE \times ARO.

Risk Register

As mentioned earlier, risk assessments should not be a one-time event. As an organization evolves, change is inevitable. Risk management needs to be part of a framework from which risk can easily be communicated and adapted on an ongoing basis.

A **risk register** gives an organization a way to record information about identified risks, and it's usually implemented as a specialized software program, cloud service, or master document. Risk registers often include enterprise- and IT-related risks. With threats and vulnerabilities identified, the organizations can then implement controls to manage the risk appropriately. (The next section discusses these techniques.) The risk register should contain specific details about the risks, especially any residual risks the organization faces as a result of

controls or mitigation techniques employed. Common contents of a risk register include the following:

- ▶ Risk categorization groupings
- ▶ Name and description of the risk
- ▶ A measure of the risk through a risk score
- ▶ The impact to the organization if the risk is realized
- ▶ The likelihood of the risk being realized
- ▶ Mitigating controls
- ▶ Residual risk
- ▶ Contingency plans that cover what happens if the risk is realized

The items listed here are fundamental components of a risk register, providing a comprehensive overview of the organization's potential and actual risk landscape. However, to address the dynamic nature of risks, and to ensure an effective and proactive approach to risk management, some other elements are crucial and warrant further exploration.

These elements, namely **key risk indicators (KRIs)**, **risk owners**, and **risk thresholds**, enhance the risk register's depth and effectiveness, ultimately providing a more nuanced understanding of the organization's risks.

KRIs function as early warning signs for potential increases in risk. By monitoring KRIs, organizations can catch and handle risk escalations before they worsen and have an impact. KRIs measure and showcase trend lines of risk exposure, offering a quantitative means to keep track of risk movements over time. These KRIs, along with other features of a risk register, are an important tool in the risk reporting process across key stakeholders.

Risk owners are individuals or teams designated with the responsibility of managing specific risks. Assigning risk owners is valuable because it not only encourages accountability but also ensures there's a specific point of contact and decision maker for each risk. It guarantees that the management of each identified risk is streamlined and focused.

Finally, **risk thresholds** help an organization determine the maximum amount of risk it can tolerate. This is a measure of the acceptable level of risk exposure for the company. Once a risk crosses its respective threshold, it calls for immediate attention. It triggers a response that could include escalated reporting, contingency plans, or mitigation strategies. Understanding risk thresholds

helps in laying out a clear roadmap for when and what action needs to be taken against the identified risks.

These items play a significant part in shaping the risk strategy of an organization and provide more context and depth to the typical components of a risk register.

ExamAlert

A risk register provides a single point of entry to record and report on information about identified risks to the organization. Ad hoc and scheduled reports from a risk register, along with KPIs and heat maps, provide useful tools for risk reporting. An organization might have one risk register for information systems and another risk register for enterprise risks, but the two are increasingly being combined.

The risk register serves as a strategic component for an organization and helps ensure that an organization's **risk appetite** and **risk tolerance** are correctly aligned with the goals of the business.

Risk Appetite and Tolerance

Risk appetite is the total amount of risk that an organization is prepared to accept or be exposed to at any point in time. It drives the organization's strategic decision-making process and is linked with the organization's objectives and strategies. Risk appetite may be categorized into three types:

- ▶ **Expansionary or aggressive:** Organizations with an expansionary risk appetite are willing to take on more risk for the potential of higher returns. These companies are often in high-growth industries where the benefits of taking a riskier approach can result in significant returns, such as tech startups and investment banking.
- ▶ **Neutral:** A company with a neutral risk appetite strikes a balance between being too risky and overly cautious. While they don't shy away from taking risks, they ensure this is done in a controlled and managed way. These organizations may be mature businesses in stable markets where business growth is consistent and returns are steady.
- ▶ **Conservative:** A conservative risk appetite involves low tolerance for risk and a preference for safer investments with predictable outcomes. These companies typically operate in highly regulated industries such as utilities and healthcare, where the emphasis is on stability, safety, and reliability rather than rapid growth.

These concepts are not unlike one's own personal behavior and risk appetite, even if subconscious. Consider, for example, your own personal values, goals, and objectives. Consider what activities you may or may not participate in, or how you personally choose to invest your savings and so forth.

Risk tolerance is the specific maximum risk that an organization is ready to handle. While risk appetite is about the overall amount of risk an organization is willing to accept, risk tolerance drills down to more specific scenarios or risk categories. Risk tolerance is the degree of variability in outcomes that an organization is willing to withstand.

For example, an organization might have a high risk tolerance for financial risks if it has strong cash reserves, but a low risk tolerance for reputational risks that could harm its brand in the marketplace.

Understanding these two concepts enables organizations to effectively manage risk in line with their strategic goals. They can select projects or make decisions that align with their appetite and tolerance for risk. The risk appetite and tolerance also guide the organization's risk management activities, determining how they identify, assess, analyze, and mitigate risk.

Together with the risk register, an organization's appetite and tolerance for risk plays an important role in helping align risk with the goals of the business. The risk register can then provide valuable information and help drive the strategic decision-making process to achieve those goals. It is important that the reporting from a risk register be clear and understandable. The outputs should be available and visible across the business, including to management and senior executives responsible for strategy, budget, and operations.

Risk Management Strategies

Risk management involves creating a risk register document that details all known risks and their related mitigation strategies. Creating the risk register involves mapping the enterprise's expected services and data sets, as well as identifying vulnerabilities in both implementation and procedures for each. Risk cannot be eliminated outright in many cases, but mitigation strategies can be integrated with policies for risk awareness training ahead of an incident. Formal risk management deals with the alignment of four potential strategies to respond to each identified risk:

- ▶ **Avoid:** Risk avoidance seeks to eliminate the vulnerability that gives rise to a particular risk. This is the most effective solution, but it often is not possible due to organizational requirements. For example, eliminating

email to avoid the risk of email-borne viruses is an effective solution but is not likely a realistic approach.

- ▶ **Transfer:** With risk transference, a risk or the effect of its exposure is transferred by moving to hosted providers that assume the responsibility for recovery and restoration. Alternatively, organizations can acquire insurance to cover the costs of equipment theft or data exposure. Insurance related to the consequences of online attacks is known as cybersecurity insurance.
- ▶ **Accept:** With risk acceptance, an organization recognizes a risk, identifies it, and accepts that it is sufficiently unlikely or of such limited impact that corrective controls are not warranted. In such cases, this is known as risk **exemption**. On the other hand, a risk **exception** is a formal acknowledgment that a system or process is not compliant with an applied standard or policy but has been permitted to operate because the risk is acknowledged and accepted. In essence, an organization agrees to tolerate a higher level of risk than usual due to unique circumstances. In most cases, these are temporary, require mitigating controls be put in place, and are given a timeline for the exception to be re-evaluated. Risk acceptance must be a conscious choice that is documented, approved by senior administration, and regularly reviewed.
- ▶ **Mitigate:** *Risk mitigation* involves reducing the likelihood or impact of a risk's exposure. Risk deterrence involves putting into place systems and policies to mitigate a risk by protecting against the exploitation of vulnerabilities that cannot be eliminated. Most risk management decisions focus on mitigation and deterrence, balancing costs and resources against the level of risk and mitigation that will result.

Bruce Schneier, a well-known cryptographer and security expert, was asked after the tragic events of 9/11 if it would be possible to prevent such events from happening again. "Sure," he replied. "Simply ground all the aircraft." Schneier gave an example of risk avoidance, albeit one he acknowledged as impractical in today's society. Consider the simple example of an automobile and its associated risks. If you drive a car, you have likely considered those risks. The option to not drive deprives you of the many benefits the car provides that are strategic to your individual goals in life. As a result, you have come to appreciate mitigating controls such as seat belts and other safety features. You accept the residual risks and might even transfer some of the risk through a life insurance policy. Certainly, when it comes to the risks of the vehicle itself, insurance plays a vital role. Not carrying insurance even carries risk

itself because insurance is often required by law. Examples abound of people who have even accepted that risk, making a conscious choice to drive without insurance.

Finally, the choices you make related to risk often result in residual risk. Living in a high-crime neighborhood might spur someone to put bars on their home's windows. That's one problem seemingly mitigated. However, in case of a fire, the bars would render common egress points in the home no longer accessible.

ExamAlert

Remember that risk can be avoided, transferred, accepted, or mitigated. Be sure you understand the different examples of when each would apply.

Risk Reporting

Risk reporting is needed for communicating risk information to stakeholders across the organization. Risk reporting involves the regular and ad hoc dissemination of risk-related information, from the operational level to senior management and the board of directors, ensuring that all parties are informed about current risks, their potential impact, and the actions taken to mitigate them. This process provides an up-to-date picture of the organization's risk profile to support strategic decision-making and help foster a proactive risk management culture.

This process benefits from the use of the risk register, which acts as a central repository of all identified risks, their assessment, and management plans. The risk register, as detailed previously, contains critical information that forms the backbone of risk reporting, which includes the following:

- ▶ Risk categorization helps in understanding the types of risks (strategic, operational, financial, compliance) the organization faces.
- ▶ Risk description and scoring provide a snapshot of each risk's nature and its relative priority.
- ▶ Impact, likelihood, and mitigation plans offer insights into the potential consequences of risks and the steps taken to manage them.
- ▶ Residual risk levels highlight the remaining risk after mitigation efforts, guiding ongoing management and monitoring.

- ▶ Key risk indicators (KRIs) and heat maps serve as visual tools for tracking and communicating risk status and trends over time.

Effective risk reporting ensures that this information is available and presented in a manner that is accessible and actionable for all stakeholders, allowing for informed discussions about risk tolerance, appetite, and strategic risk management priorities. Risk reports should not only highlight where risks align or deviate from the organization's risk appetite but also signal when risk levels approach or exceed predefined tolerance thresholds. This alignment ensures that risk management efforts are strategic, targeted, and effective in supporting the organization's objectives.

Business Impact Analysis

Business impact analysis (BIA) is the process of determining the potential impacts resulting from the interruption of time-sensitive or critical business processes. IT risk assessment, as well as planning for both disaster recovery and operational continuity, relies on conducting a BIA as part of the overall plan to ensure continued operations and the capability to recover from disaster. The BIA focuses on the relative impact of the loss of operational capability on critical business functions. Conducting a business impact analysis involves identifying critical business functions and the services and technologies required for them, along with determining the associated costs and the maximum acceptable outage period.

For hardware-related outages, the assessment should also include the current age of existing solutions, along with standards for the expected average time between failures, based on vendor data or accepted industry standards. Planning strategies are intended to minimize this cost by arranging recovery actions to restore critical functions in the most effective manner based on cost, legal or statutory mandates, and calculations of the mean time to restore.

A business impact analysis is a key component in ensuring continued operations. For that reason, it is a major part of a business continuity plan (BCP) or continuity of operations plan (COOP) as well. The focus is on ensuring the continued operation of key mission and business processes. U.S. government organizations commonly use the term mission-essential functions to refer to functions that need to be immediately functional at an alternate site until normal operations can be restored. Essential functions for any organization require resiliency. Organizations also must identify the dependent systems for both the functions and the processes that are critical to the mission or business.

A BCP must identify critical systems and components. If a disaster is widespread or targets an Internet service provider (ISP) or key routing hardware point, an organization's continuity plan should detail options for alternate network access. This should include dedicated administrative connections that might be required for recovery. Continuity planning should include considerations for recovery in case existing hardware and facilities are rendered inaccessible or unrecoverable. It should also consider the hardware configuration details, network requirements, and utilities agreements for alternate sites.

RTO and RPO

Recovery point objective (RPO) and **recovery time objective (RTO)** are important concepts of the BCP and form part of the broader risk management strategy. RPO, which specifically refers to data backup capabilities, is the amount of time that can elapse during a disruption before the quantity of data lost during that period exceeds the BCP's maximum allowable threshold. Simply put, RPO specifies the allowable data loss. It determines up to what point in time data recovery can happen before business is disrupted. For example, if an organization does a backup at 10:00 p.m. every day and an incident happens at 7:00 p.m. the following day, everything that changed since the last backup would be lost. The RPO in this context is the backup from the previous day. If the organization set the threshold at 24 hours, the RPO would be within the threshold because it is less than 24 hours.

The RTO is the amount of time within which a process must be restored after a disaster to meet business continuity requirements. The RTO is how long the organization can go without a specific application; it defines how much time is needed to recover after a notification of process disruption.

ExamAlert

Be certain that you understand the distinction between RPO and RTO. RPO designates the amount of data that will be lost or will have to be re-entered because of network downtime. RTO designates the amount of time that can pass before the disruption begins to seriously impede normal business operations.

MTTF, MTBF, and MTTR

When systems fail, one of the first questions asked is, "How long will it take to get things back up?" It is better to know the answer to such a question *before* disaster strikes than to try to find the answer afterward. Fortunately, established

mechanisms can help you determine this answer. Understanding these mechanisms is a big part of the overall analysis of business impact.

Mean time to failure (MTTF) is the length of time a device or product is expected to last in operation. It represents how long a product can reasonably be expected to perform, based on specific testing. MTTF metrics supplied by vendors about their products or components might not have been collected by running one unit continuously until failure. Instead, MTTF data is often collected by running many units for a specific number of hours and then is calculated as an average based on when the components fail.

MTTF is one of many ways to evaluate the reliability of hardware or other technology and is extremely important when evaluating mission-critical systems hardware. Knowing the general reliability of hardware is vital, especially when it is part of a larger system. MTTF is used for nonrepairable products. When MTTF is used as a measure, repair is not an option.

Mean time between failures (MTBF) is the average amount of time that passes between hardware component failures, excluding time spent repairing components or waiting for repairs. MTBF is intended to measure only the time a component is available and operating. MTBF is similar to MTTF, but it is important to understand the difference. MTBF is used for products that can be repaired and returned to use. MTTF is used for nonrepairable products. MTBF is calculated as a ratio of the cumulative operating time to the number of failures for that item.

MTBF ratings can be predicted based on product experience or data supplied by the manufacturer. MTBF ratings are measured in hours and are often used to determine the durability of hard drives and printers. For example, typical hard drives for personal computers have MTBF ratings of about 500,000 hours.

These risk calculations help determine the life spans and failure rates of components. These calculations help an organization measure the reliability of a product.

One final calculation assists with understanding approximately how long a repair will take on a component that can be repaired. The **mean time to repair (MTTR;** also called mean time to recovery) is the average time required to fix a failed component or device and return it to production status. MTTR is corrective maintenance. The calculation includes preparation time, active maintenance time, and delay time. Because of the uncertainty of these factors, MTTR is often difficult to calculate. In order to reduce the MTTR, some systems have redundancy built in so that when one subsystem fails, another takes its place and keeps the whole system running.

ExamAlert

Mean time between failures (MTBF) is the average time before a product requires repair. Mean time to repair (MTTR) is the average time required to fix a failed component or device and return it to production status. On the other hand, mean time to failure (MTTF) is the average time before a product fails and cannot be repaired. MTBF and MTTR consider a component that can be repaired, whereas MTTF considers a component that cannot be repaired.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this chapter again until you can.

1. Which of the following is the monetary loss that can be expected for an asset from risk over a year?
 - A. ALE
 - B. SLE
 - C. ARO
 - D. BIA
2. Your manager needs to know, for budgetary purposes, the average life span for each of the firewall appliances. Which of the following should you provide?
 - A. MTBF
 - B. RPO
 - C. RTO
 - D. MTTF
3. An organization is increasingly subject to compliance regulations and is making strong efforts to comply with them but is still concerned about issues that might occur. Management decides to buy insurance to help cover the costs of a potential breach. Which of the following risk response techniques is the organization using?
 - A. Avoidance
 - B. Transference
 - C. Acceptance
 - D. Mitigation

4. Which of the following equations best represents the proper assessment of exposure to danger?
- A. $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$
 - B. $\text{Impact} = \text{Risk} \times \text{Threat} \times \text{Vulnerability}$
 - C. $\text{Vulnerability} = \text{Threat} \times \text{Risk} \times \text{Impact}$
 - D. $\text{Threat} = \text{Risk} \times \text{Impact} \times \text{Vulnerability}$
5. A security analyst needs a single point of entry to record information about identified risks to his organization. What will allow him to do this?
- A. ALE
 - B. Risk register
 - C. SLE
 - D. ARO
6. Which type of risk assessment uses a risk matrix/heatmap that plots the probability of risks using a scale of low, medium, or high?
- A. Quantitative
 - B. Adversarial
 - C. Qualitative
 - D. Environmental
7. If a single loss expectancy is \$25,000 and the annual rate of occurrence is .5, what is the annual loss expectancy?
- A. \$12,500
 - B. \$25,000
 - C. \$5,000
 - D. \$2,500

Cram Quiz Answers

Answer 1: A. The annual loss expectancy (ALE) is the monetary loss that can be expected for an asset from risk over a 1-year period. It is calculated by multiplying the single loss expectancy by the annual rate of occurrence (that is, $\text{SLE} \times \text{ARO}$). Therefore, answers B and C are incorrect. Answer D is incorrect because this is a business impact analysis, which is the process for determining potential impacts resulting from the interruption of business processes.

Answer 2: D. The mean time to failure (MTTF) is the length of time a device or product is expected to last in operation. It represents how long a product can reasonably be expected to perform, based on specific testing. Answer A is incorrect because the mean time between failures (MTBF) is the average amount of time that passes between

hardware component failures, excluding time spent repairing components or waiting for repairs. Answers B and C are incorrect because RPO and RTO are used for risk-mitigation planning. The recovery point objective (RPO) specifies the allowable data loss. The recovery time objective (RTO) is the amount of time within which a process must be restored after a disaster to meet business continuity requirements.

Answer 3: B. Insurance is a classic example of transferring risk. Answers A, C, and D are incorrect because none of them transfers the risk from one organization to another.

Answer 4: A. Risk is a function of threats, vulnerabilities, and potential impact. Assessing the level of risk is often portrayed through the simple equation $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$. Answers B, C, and D are incorrect because threat, vulnerability, and impact are considered together to provide an appropriate measure of risk.

Answer 5: B. A risk register is a strategic component for organizations. The register also helps ensure that an organization's risk tolerance and appetite are correctly aligned with the goals of the business. A risk register provides a single point of entry to record information about identified risks to the organization. Answer A is incorrect because the annual loss expectancy (ALE) is the monetary loss that can be expected for an asset from risk over a one-year period. Answer C is incorrect because single loss expectancy (SLE) is the expected monetary loss every time a risk occurs. Answer D is incorrect because the annual rate of occurrence (ARO) is the estimated possibility of a specific threat taking place in a 1-year time frame.

Answer 6: C. Qualitative risk assessment can involve brainstorming, focus groups, surveys, and other similar processes to determine asset worth and valuation to the organization. Uncertainty is also estimated, allowing for a relative projection of qualitative risk for each threat, based on its position in a risk matrix/heat map that plots the probability (very low to very high) and impact (very low to very high). Numeric values can be assigned to each state (very low = 1, low = 2, moderate = 3, and so on) to perform a quasi-quantitative analysis, but because the categories are subjectively assigned, the result remains qualitative. Answer A is incorrect because a quantitative assessment is less subjective, and the process requires assigning a value to all the various components. To perform a quantitative risk assessment, an estimation of potential losses is calculated. Answers B and D are incorrect because these terms describe threat source types, which can be adversarial, accidental, structural, or environmental, for example.

Answer 7: A. The annual loss expectancy (ALE) is the monetary loss that can be expected for an asset from risk over a 1-year period. ALE equals the single loss expectancy (SLE) times the annual rate of occurrence (ARO): that is, $\text{SLE} \times \text{ARO} = \text{ALE}$. So, if the SLE is \$25,000 and the ARO is .5, the ALE is \$12,500 (that is, $\$25,000 \times .5 = \$12,500$). Therefore, Answers B, C, and D are incorrect.

What Next?

If you want more practice on this chapter's exam objective before you move on, remember that you can access all of the Cram Quiz questions on the Pearson Test Prep software online. You can also create a custom exam by objective with the Online Practice Test. Note any objective you struggle with and go to that objective's material in this chapter.

This page intentionally left blank

Index

Numbers

3DES (Triple DES), 166

802.1X, 221, 288–289

A

AAA framework, 13–14, 286–287

ABAC (attribute-based access control), 387–388

acceptable use policy (AUP), 433–435

acceptance of risk, 476

access badges, 21

access control, 386–388. *See also* identity and access management

AAA framework, 13–14, 286–287

access badges, 21

access logs, 333

ACLs (access control lists), 12, 162–163, 352

deception and disruption technology, 23

overview of, 162–164

permissions, 164

physical security, 18–23

policy-driven, 16–17

standards, 446

vestibules, 19

Zero Trust, 15–18

access logs, 333

accounting, 14, 297

acknowledgement, 500

ACLs (access control lists), 12, 162–163, 352

acquisition, 296, 414

active devices, 215–216, 229

active reconnaissance, 516–517

activity monitoring, 332–336

alert response and remediation/

activity monitoring

- validation, 335
- alert tuning, 336
- alerting, 333
- archiving, 334–335
- log aggregation, 332–333
- quarantine, 335
- reporting, 334
- scanning, 334
 - rescanning, 325–326
 - URL scanning, 360
 - vulnerability scans, 308–309, 421

ad hoc risk assessments, 467**adaptation, security awareness programs, 547****adaptive identity, 16****Advanced Encryption Standard (AES), 166, 259, 367****advanced persistent threats (APTs), 89****adversary tactics, techniques, and procedures (TTPs), 312****AES (Advanced Encryption Standard), 166, 259, 367****agent-based tools, 337****agent-based web filters, 358****agentless tools, 337****aggregation, log, 332–333****aggressive risk appetite, 474****agreement types, 489–491****air gaps, 189–190****AIS (automated indicator sharing), 312****ALE (annual loss expectancy), 472****alerts, 333**

- alert mechanisms, 543
- response and remediation/validation, 335
- tuning, 336

algorithms, cryptographic

- asymmetric, 53–55
- definition of, 43
- key exchange, 50
- key length, 50–51
- key stretching, 49–50
- overview of, 49–50
- symmetric, 51–53

allow lists, 32, 164**Amazon Web Services, 185****American National Standards Institute (ANSI), 20****amplified DDoS (distributed denial-of-service), 141–142****analysis**

- dynamic, 310
- incident, 410
- risk, 468–472
 - ALE (annual loss expectancy), 472
 - ARO (annual rate of occurrence), 471–472
 - qualitative, 469–470
 - quantitative, 470
 - SLE (single loss expectancy), 470–471
 - steps for, 468–469
 - SDLC (software development lifecycle)
 - policy, 441
 - static, 290, 310
 - vulnerability management, 316–317

annual loss expectancy (ALE), 472**annual rate of occurrence (ARO), 471–472****anomalous behavior recognition, 532–533****anomaly-based IDSs/IPSSs, 218****ANSI (American National Standards Institute), 20****antimalware, 271, 274****antivirus tools, 274, 341****APIs (application programming interfaces), 405****appetite for risk, 474–475****appliances, network**

- definition of, 216
- IDS (intrusion detection system), 218–219, 229
- IPS (intrusion prevention system), 218–219, 229
- jump servers, 216–217, 229
- load balancers, 219, 229
- proxy servers, 217–218, 229
- sensors, 220, 229

- application allow lists, 164**
- application attacks, 148–153**
 - buffer overflow, 149–150
 - directory traversal, 152–153
 - forgery, 151–152
 - injection, 148–149
 - privilege escalation, 150
 - replay attacks, 150
- application logs, 420**
- application monitoring, 330–331**
- application programming interfaces (APIs), 405**
- application restart, 33**
- application security, 289–290, 309–311**
- application vulnerabilities, 116–118**
- approval process, change management, 29**
- archiving, 334–335**
- ARO (annual rate of occurrence), 471–472**
- assessments**
 - assessment quizzes, 546
 - attestation, 510–511
 - external, 512–513
 - internal, 511–512
 - overview of, 510
 - penetration testing
 - components of, 514–515
 - defensive, 519
 - environments for, 520–521
 - integrated, 519
 - offensive, 518
 - overview of, 513–516
 - phases of, 515–516
 - physical tests, 517–518
 - reconnaissance, 516–517
 - risk, 466–468
 - self-assessments, 512
 - vendor, 486–488
- asset management. See data asset management**
- asset tracking, 299**
- assignment/accounting, 297**
- asymmetric algorithms, 51–53**
- asynchronous replication, 260**
- attack phase, penetration testing, 516**
- attack surfaces, 98, 214, 229**
- attestation, 56, 385–386, 500, 510–511**
- attribute-based access control (ABAC), 387–388**
- attributes, device, 215–216**
- audit committees, 512**
- audit logs, 332**
- audits, 326**
 - attestation, 510–511
 - audit committees, 512
 - external, 512–513
 - internal, 511–512
 - logs, 332
 - overview of, 510
 - penetration testing
 - components of, 514–515
 - defensive, 519
 - environments for, 520–521
 - integrated, 519
 - offensive, 518
 - overview of, 513–516
 - phases of, 515–516
 - physical tests, 517–518
 - reconnaissance, 516–517
 - routine, 544
 - system or process audits, 316
- AUP (acceptable use policy), 433–435**
- authentication, 14**
 - device hardening, 271
 - passwordless, 397
 - protocols, 288–289
 - tokens, 391–393
 - workstations, 271
- authorization, 14**
- automated indicator sharing (AIS), 312**
- automation and orchestration**
 - benefits of, 405–406
 - compliance and, 500
 - considerations for, 406–407

- reports, 421
- use cases, 402–405

availability, 12–13, 202

avoidance of risk, 475–476

awareness. See security awareness

awareness, user training for, 535–536

Azure, 185

B

backout plans, 30

backups, 255–258

- definition of, 255–256
- differential, 256
- frequency of, 258
- full, 256
- incremental, 256
- onsite/offsite, 257

badges, access, 21

bare-metal hypervisors, 196–197

baselines, 268–269

BCPs (business continuity plans), 205, 437–438, 478

BDPU (Bridge Protocol Data Unit) Guard, 221

BEC (business email compromise), 109–110

benchmarks, 337

BIA (business impact analysis), 467, 478–479

biometrics, 389–391

birthday attacks, 154

Bitcoin, 66–67

BitLocker, 45

blackmail, threat actors motivated by, 92

block ciphers, 52

block rules, 360–361

blockchain, 66–67

block/deny lists, 164

Bluetooth, 285

- unsecured, 104
- wireless network attacks, 146

boards, 431

boatware, 135

bollards, 19

BPAs (business partner agreements), 490

brand impersonation, 111

Bridge Protocol Data Unit (BDPU) Guard, 221

bring your own device (BYOD), 282–283

brute-force attacks, 138, 155

buffer overflow, 116, 149–150

bug bounty programs, 316

business continuity plans (BCPs), 205, 437–438, 478

business email compromise (BEC), 109–110

business impact analysis (BIA), 467, 478–479

business partner agreements (BPAs), 490

business processes impacting security operations, 28–31

BYOD (bring your own device), 282–283

bypassing security controls, 315, 514

C

cables, removable, 538–539

California Consumer Privacy Act (CCPA), 454, 502, 504

capacity planning, 253–254

CAs (certificate authorities), 66, 69–70

CAs (corrective actions), 413

CASB (cloud access security broker), 228

CCM (Cloud Controls Matrix), 459

CCPA (California Consumer Privacy Act), 454, 502, 504

cellular networks, 284

centralized architectures, 192–193

centralized proxies, 359–360

centralized structures, 431

certificate revocation lists (CRLs), 77

certificate signing requests (CSRs), 72

certificates, 67–68

- CAs (certificate authorities), 66, 69–70
- CPS (certification practice statement), 70–71
- CRLs (certificate revocation lists), 77
- CSRs (certificate signing requests), 72
- formats, 75–76
- OCSP stapling, 78
- pinning, 79
- policy, 72–73
- revocation of, 77
- trust models, 71–72
- types of, 73–75

certification

- certification attestation, 511
- CPS (certification practice statement), 70–71
- data asset management, 302

chain of custody, 414

change management

- business processes impacting security operations, 28–31
- documentation, 35–36
- overview of, 28
- policy, 443–444
- technical implications, 31–34
- version control, 36

chaos, threat actors motivated by, 93–94

choose your own device (CYOD), 283

CIA (confidentiality, integrity, and availability), 12–13, 237

Cisco TALOS, 313

classifications

- data, 237–238, 297
- vulnerability, 320

client-based software, 103

cloning attacks, 138

cloud computing

- CASBs (cloud access security brokers), 228
- definition of, 180–181
- hybrid considerations, 184–185
- IaC (Infrastructure as code), 186–187

- multicloud systems, 252
- responsibility matrix, 181–183
- securing, 273–274
- third-party vendors, 185–186
- vulnerabilities, 122–123

Cloud Controls Matrix (CCM), 459

Cloud Security Alliance (CSA), 459

clustering, 248–249

COBIT (Control Objectives for Information and Related Technology), 459

COBO (corporate owned, business only), 283

code repositories, 313

code signing, 74, 290

cold sites, 250

collision attacks, 153–154

Committee of Sponsoring Organizations (COSO), 459

committees, 431, 512

Common Vulnerability Scoring System (CVSS), 318–322

commonly used ports, 172

communication encryption, 48–49

compensating controls, 6–7, 324

complexity

- of automation and orchestration, 406
- of passwords, 395–396

compliance

- audits, 511–512
- consequences of noncompliance, 497–498
- internal/external, 496–497
- monitoring, 499–501
- overview of, 496
- privacy
 - data inventory and retention, 503–504
 - definition of, 501
 - legal implications of, 504–505
 - privacy data roles, 501–503
 - right to be forgotten, 505
- reporting, 496–497

computer resource monitoring

computer resource monitoring. *See* resource monitoring

confidential data, 238, 298

confidentiality, 12–13

configuration
 enforcement, 167–168
 errors, 118

conflict of interest, 489

connection methods, 283–285

connectivity, enterprise architecture security, 214, 229

conservative risk appetite, 474

consistent training, 544

containerization, 193–195

containment phase, incident response, 410

content categorization, 360

content development, 545–546

continuity of operations plan (COOP), 205, 252–253, 478

continuous integration and testing, 404–405

continuous risk assessments, 468

contractual impacts of non-compliance, 498

control apps, 271

Control Objectives for Information and Related Technology (COBIT), 459

control plane, 16

controllers, 460, 503

cookies, 290

COOP (continuity of operations plan), 205, 252–253, 478

COPE (corporate owned, personally enabled), 283

corporate owned, business only (COBO), 283

corrective actions (CAs), 413

corrective controls, 6

COSO (Committee of Sponsoring Organizations), 459

cost
 automation and orchestration, 406–407
 network infrastructure, 203

CPS (certification practice statement), 70–71

credentials
 credential replay, 147
 default, 105

critical data, 238

Critical vulnerabilities, 320

CRL (certificate revocation list), 77

cross-site scripting (XSS), 120, 148–149

CrowdStrike Falcon X, 313

cryptographic attacks, 153–154

cryptographic erasure, 302

Cryptographic Message Syntax, 367

cryptography. *See also* encryption
 algorithms
 asymmetric, 53–55
 key exchange, 50
 key length, 50–51
 key stretching, 49–50
 overview of, 49–50
 symmetric, 51–53

blockchain, 66–67

digital certificates, 67–68
 CAs (certificate authorities), 69–70
 CPSs (certification practice statements), 70–71
 CSRs (certificate signing requests), 72
 formats, 75–76
 OCSP stapling, 78
 pinning, 79
 policy, 72–73
 revocation of, 77
 trust models, 71–72
 types of, 73–75

digital signatures, 64–66

key escrow, 431

OCSP stapling, 78

open public ledger, 67

PKI (public key infrastructure), 428–429

protocols, 287–288

public/private keys, 430–431

tools

- HSM (hardware security module), 57–58
- KMS (key management system), 58
- secure enclave, 58
- TPM (Trusted Platform Module), 55–57

vulnerabilities, 125–126

CSA (Cloud Security Alliance), 459**CSR (certificate signing request), 72****custodians, 460–461****custody, chain of, 414****CVE Details, 312****CVSS (Common Vulnerability Scoring System), 318–322****CWE, 320****CYOD (choose your own device), 283****D****DAC (discretionary access control), 387****dark web, 314****dashboards, 421****data asset management**

- acquisition/ procurement process, 296
- assignment/accounting, 297
- certification, 302
- classification, 297–299
- data classifications, 237–238
- data inventory and retention, 503–504
- data retention, 303
- destruction, 302
- disposal/decommissioning, 300–301
- enumeration, 300
- inventory, 300
- monitoring/asset tracking, 299
- ownership, 297
- sanitization, 301–302

data at rest, 59**data controllers, 460, 503****data exfiltration, threat actors motivated by, 90–91****data in transit, 59, 239****data in use, 59, 239****data loss prevention (DLP) software, 341–342, 369, 370–371, 532****data masking, 60–61, 242****data obfuscation, 242**

- data masking, 60–61
- hashing, 63–64
- overview of, 59–62
- redaction, 61
- salting, 63–64
- steganography, 62–63
- tokenization, 60

data ownership, 502**data plane, 16****data privacy. See privacy compliance****data processors, 503****data protection**

- data classifications, 237–238
- data security methods, 240–243
- data sovereignty, 239–240
- data states, 239
- data types, 234–237
- geolocation, 240

data roles, 501–503**data segmentation, 243****data sources for investigation support**

- automated reports, 421
- dashboards, 421
- log data, 419–421
- packet captures, 422
- vulnerability scans, 421

data sovereignty, 239–240**data states, 239****data subjects, 502****data types, 234–237****data wiping, 301****databases, 47****DDoS (distributed denial-of-service), 140–142****dead zones, 279****decentralized architectures, 192–193, 431**

- deception and disruption technology, 23
- decommissioning, 300–301
- default credentials, 105
- defensive penetration testing, 519
- degaussing, 301
- demilitarized zone (DMZ), 353–354
- denial-of-service (DoS) attacks, 171
- deny lists, 32
- dependencies, 34
- deployment, 204, 282–283, 442
- DER (distinguished encoding rules), 76
- design phase, SDLC (software development lifecycle) policy, 441
- destruction, 302
- detection phase, incident response, 410
- deterrent controls, 5
- development
 - SDLC (software development lifecycle) policy, 441
 - security awareness programs, 545–547
- device attributes, 215–216
- device placement, 228
- DHCP (Dynamic Host Configuration Protocol) snooping, 221
- diagrams, updating, 35
- differential backups, 256
- digital certificates, 67–68
 - CAs (certificate authorities), 66, 69–70
 - CPSs (certification practice statements), 70–71
 - CSRs (certificate signing requests), 72
 - formats, 75–76
 - OCSP stapling, 78
 - pinning, 79
 - policy, 72–73
 - revocation of, 77
 - trust models, 71–72
 - types of, 73–75
- digital forensics, 414–415
- digital signatures, 64–66, 241
- directive controls, 7
- directory traversal, 152–153
- disabling ports/protocols, 171–172
- disaster recovery plans (DRPs), 205, 438–440
- discovery phase, penetration testing, 515–516
- discretionary access control (DAC), 387
- disinformation, 108–109
- dispersion, geographic, 251
- disposal/decommissioning, 300–301
- disruption/chaos, threat actors motivated by, 93–94
- distinguished encoding rules (DER), 76
- distributed denial-of-service (DDoS), 140–142
- diversity, platform, 251
- DKIM (DomainKeys Identified Mail), 368
- DLL injection, 149
- DLP (data loss prevention), 341–342, 369, 370–371
- DMARC (Domain-based Message Authentication, Reporting, and Conformance), 369
- DNS (Domain Name System), 364, 365
 - attacks, 142–144
 - filtering, 366
- documentation, 35–36
- domain hijacking, 142–143
- Domain Name System. *See* DNS (Domain Name System)
- domain validation (DV), 73
- Domain-based Message Authentication, Reporting, and Conformance (DMARC), 369
- DomainKeys Identified Mail (DKIM), 368
- DoS (denial-of-service) attacks, 171
- downgrade attacks, 153
- downtime, 32–33
- DRPs (disaster recovery plans), 205, 438–440
- dual power supply units (PSUs), 261
- due care, 499–501
- due diligence, 488–489, 499–501
- Duronio, Roger, 136–137
- DV (domain validation), 73

dynamic analysis, 310

Dynamic Host Configuration Protocol (DHCP) snooping, 221

dynamic/private ports, 171

E

EAP (Extensible Authentication Protocol), 221, 229, 288–289

ease of deployment, 204

ease of recovery, 205

e-discovery, 415

EDR (endpoint detection and response), 169, 330, 372–373

EFS (Encrypting File System), 45

EK (endorsement key), 56

email, 99–100

encryption, 369

phishing, 107–108

components of, 526–528

lessons from, 528

recognizing, 528–530

responding to, 530–531

security, 367–369

embedded systems, 200–201, 276

Encrypting File System (EFS), 45

encryption, 12, 166, 241, 258–259

algorithms, 43–44

asymmetric, 53–55

definition of, 43

key exchange, 50

key length, 50–51

key stretching, 49–50

overview of, 49–50

symmetric, 51–53

blockchain, 66–67

cloud infrastructure, 273

communication, 48–49

cryptographic protocols, 287–288

data obfuscation

data masking, 60–61

hashing, 63–64

overview of, 59–62

redaction, 61

salting, 63–64

steganography, 62–63

tokenization, 60

definition of, 43–44

device hardening, 271

digital certificates, 67–68

CAs (certificate authorities), 66, 69–70

certificate formats, 75–76

certificate policy, 72–73

certificate types, 73–75

CPSs (certification practice statements), 70–71

CSRs (certificate signing requests), 72

OCSP stapling, 78

pinning, 79

revocation of, 77

trust models, 71–72

digital signatures, 64–66

email, 369

file-level, 44–45

full-disk, 44

hardening with, 168–169

levels and types, 44–48

mobile solutions, 281

OCSP stapling, 78

open public ledger, 67

RTOS (Real-Time Operating System), 277

servers, 274

standards, 446

tools

HSM (hardware security module), 57–58

KMS (key management system), 58
secure enclave, 58

TPM (Trusted Platform Module), 55–57

transport, 48–49

workstations, 272

end of service life (EOL) date, 492

end-of-life (EoL), 121, 492

endorsement key (EK), 56

endpoint detection and response (EDR)

endpoint detection and response (EDR), 169, 330, 372–373

endpoint logs, 420

endpoint protection, 169, 271

engagement, rules of, 492–493

engaging content, creating, 545–546

ENISA (European Union Agency for Network and Information Security), 456

enterprise architecture

attack surfaces, 214, 229

connectivity, 214, 229

device attributes, 215–216

failure modes, 214–215, 229

firewalls, 222–224, 229

access lists, 352

ports/protocols, 352

rules, 350–351

infrastructure considerations, 212

network appliances

definition of, 216

jump servers, 216–217, 229

proxy servers, 217–218, 229

port security, 220–222, 229

remote access, 225–226

SASE (Secure Access Service Edge), 228

SD-WAN (software-defined wide area network), 227–228, 230

security zones, 213, 228

selection of effective controls, 228–230

tunneling, 226–227

VPNs (virtual private networks), 225

enterprise security capabilities

DLP (data loss prevention), 370–371

DNS filtering, 366

EDR (endpoint detection and response), 372–373

email security, 367–369

FIM (File Integrity Monitoring), 369–370

firewalls, 350–353

IDS/IPS, 354–356

NAC (network access control), 371–372

operating system security, 361–363

screened subnets, 353–354

secure protocol implementation, 363–366

port selection, 365

protocol selection, 364

transport method, 365–366

UBA (user behavior analytics), 373

web filters, 357–361

XDR (extended detection and response), 372–373

enumeration, data asset management, 300

environmental attacks, 139

environmental penetration testing, 520–521

environmental variables, 321

EOL (end of life), 121, 492

ephemeral credentials, 398

eradication phase, incident response, 411

escalation of tickets, 403–404

escrow, key, 431

espionage, threat actors motivated by, 91

ethical motivations of threat actors, 93

EU Digital Services Act, 498

European Union Agency for Network and Information Security (ENISA), 456

EV (extended validation), 74

examinations, 513

exceptions, 324–325

exchange, key, 50

Execute permissions, 381

execution, security awareness programs, 545–547

exemptions, 324–325

expansionary risk appetite, 474

expiration of passwords, 396

exploiting vulnerabilities, 315, 515

exposure factors, 321

- extended detection and response (XDR), 372–373
 - extended validation (EV), 74
 - Extensible Access Control Markup Language (XACML), 387–388
 - Extensible Authentication Protocol (EAP), 221, 229, 288–289
 - external audits and assessments, 512–513
 - external compliance, 497
 - external considerations, 453–455
 - external monitoring, 500
 - external threats, 84
- ## F
-
- facial recognition, 390
 - factors, identity and access management, 394–395
 - fail-closed, 215, 229
 - fail-open, 214–215, 229
 - failover testing, 255
 - failure modes, enterprise architecture security, 214–215, 229
 - false acceptance rate (FAR), 391
 - false negatives, 317
 - false positives, 317
 - false rejection rate (FRR), 391
 - FDE (full disk encryption), 45
 - Federal Identity, Credential, and Access Management (FICAM) Roadmap, 387–388
 - fencing, 20
 - File Integrity Monitoring (FIM), 369–370
 - File Transfer Protocol (FTP), 364, 365
 - file-based threat vectors, 101
 - file/code repositories, 313
 - file-level encryption, 44–45
 - filtering
 - DNS, 366
 - gateways, 369
 - MAC, 280
 - web, 357–361
 - FIM (File Integrity Monitoring), 369–370
 - financial information, 236
 - financial motivations of threat actors, 92
 - Financial Services Information Sharing and Analysis Center (FS-ISAC), 313–314
 - finest, noncompliance, 498
 - fingerprint biometrics, 390
 - firewalls, 222–224, 229, 350–353
 - access lists, 352
 - FWaaS (firewall as a service), 228
 - host-based, 170
 - Layer 4/Layer 7, 224, 230
 - logs, 420
 - NGFWs (next-generation firewalls), 223–224, 230
 - ports/protocols, 352
 - rules, 350–351
 - secure communication/access, 224–225
 - UTM (unified threat management), 223, 230
 - WAF (web application firewall), 222–223, 229
 - firmware, 120–121
 - flooding
 - ping, 140
 - SYN, 141
 - forensics, digital, 414–415
 - forgery, 151–152
 - forward proxy servers, 217–218
 - fraffle attacks, 140
 - frequency of backups, 258
 - FRR (false rejection rate), 391
 - FS-ISAC (Financial Services Information Sharing and Analysis Center), 313–314
 - FTM (File Integrity Monitoring), 369–370
 - FTP (File Transfer Protocol), 364, 365
 - full backups, 256
 - Full Control permissions, 379–381
 - full disk encryption (FDE), 45
 - full-disk encryption, 44
 - FWaaS (firewall as a service), 228

G

gait biometrics, 390

Galois/Counter Mode Protocol, 288

gap analysis, 14–15

gates, 20

gateways, 369

GDPR (General Data Protection Regulation), 234, 455, 497, 502, 504

generators, 262

geographic dispersion, 251

geographic restrictions, 240–241

geolocation, 240

GLBA (Gramm-Leach-Bliley Act), 235, 455

global data privacy, 504

goals, identifying, 545

Google Cloud Platform, 185

governance. See also policies

external considerations, 453–455

governing framework, 428–429

guidelines, 428, 452–453

industry-specific framework, 458–460

monitoring, 432–433

procedures, 429, 447–452

regulatory and nonregulatory requirements, 455–458

revision, 432–433

roles and responsibilities, 460–462

standards, 428, 445–447

structures, 430–431

governing framework, 428–429

government entities, 431

GPOs (Group Policy Objects), 362

Gramm-Leach-Bliley Act (GLBA), 235, 455

Group Policy, 361–362

groups, 381, 403

guard rails, 403

guidelines, 428, 452–453

H

hacktivists, 87

hand geometry, 390

handbooks, user guidance and training, 534–535

hard authentication tokens, 391–393

hardening techniques, 270

default password changes, 173

definition of, 168

encryption, 168–169

endpoint protection, 169

HIPS (host-based intrusion prevention system), 170

host-based firewalls, 170

ports/protocols, disabling, 171–172

removal of unnecessary software, 173–174

hardware providers, 124–125

hardware security module (HSM), 57–58

hardware vulnerabilities, 120–121

hashing, 63–64, 241

Health Information Sharing and Analysis Center (Health-ISAC), 313–314

Health Information Trust Alliance Common Security Framework (HITRUST CSF), 459

Health Insurance Portability and Accountability Act (HIPAA), 235, 454, 455, 457

heat maps, 278

heuristic-based analysis, 219

high availability, 202, 248–249

High vulnerabilities, 320

hijacking, domain, 142–143

HIPAA (Health Insurance Portability and Accountability Act), 235, 454, 455, 457, 504

HIPS (host-based intrusion prevention system), 170

HITRUST CSF (Health Information Trust Alliance Common Security Framework), 459

HMAC-based one-time password (HOTP), 392

honeyfiles, 23

honeynets, 23

honeypots, 23

honeytokens, 23

host-based firewalls, 170

host-based intrusion prevention system (HIPS), 170
hosted hypervisors, 196–197
hot sites, 250
hotfixes, 323
HOTP (HMAC-based one-time password), 392
HPKP (HTTP Public Key Pinning), 79
HSM (hardware security module), 57–58
HTTP (Hypertext Transfer Protocol), 364, 365
HTTP Public Key Pinning (HPKP), 79
human vectors, 106–112
human-readable data, 236–237
hybrid cloud considerations, 184–185
hybrid work environments, 541–542
Hypertext Transfer Protocol (HTTP), 364, 365
hypervisors, 196–197

I

laaS (infrastructure as a service), 181
laC (Infrastructure as code), 186–187
ICS (Industrial Control Systems), 198–199, 275
identification methods, 308
identity and access management
 access controls, 386–388
 attestation, 385–386
 factors, 394–395
 identity proofing, 381–382
 implementations, 389–398
 biometrics, 389–391
 hard/soft authentication tokens, 391–393
 security keys, 393–394
 interoperability, 385
 MFA (multifactor authentication), 388–398
 password concepts, 395–397
 password managers, 397
 passwordless authentication, 397
 permissions assignment, 379–381
 privileged access management tools, 397–398
 provisioning/de-provisioning user accounts, 378–379
 SSO (single sign-on), 382–385
identity proofing, 381–382
IDS (intrusion detection system), 216, 218–219, 229, 354–356
 signatures, 356
 trends in, 355–356
IEEE 802.1X, 221
IM (instant messaging), 100–101
IMAP (Internet Message Access Protocol), 364, 365
immediate response, 543
impact analysis, 30
impersonation, 109
implementations, identity and access management, 389–398
 biometrics, 389–391
 hard/soft authentication tokens, 391–393
 security keys, 393–394
incident response
 digital forensics, 414–415
 phishing attempts, 530–531
 policy, 440–441
 process for, 410–411
 RCA (root cause analysis), 412–413
 threat hunting, 413
 training and testing, 411–412
incremental backups, 256
independent assessments, 487–488
independent third-party audits, 513
indicators of compromise (IOCs), 169, 312, 413
indicators of malicious activity, 156–157
Industrial Control Systems (ICS), 198–199, 275
industry/organizational impact, vulnerability management, 321–322
industry-specific framework, 458–460
influence campaigns, 108–109
information security policy, 435–437

- Information Sharing And Analysis Centers (ISACs), 313–314**
 - Informational vulnerabilities, 320**
 - information-sharing organizations, 313–314**
 - infrared sensors, 22**
 - infrastructure**
 - capacity planning for, 254
 - IaaS (infrastructure as a service), 181
 - IaC (Infrastructure as code), 186–187
 - monitoring, 331–332
 - Initiative for Open Authentication (OATH), 392**
 - injection, 148–149**
 - DLL, 149
 - LDAP, 149
 - SQL, 149
 - XML, 149
 - inline devices, 216, 229**
 - input validation, 289**
 - insider threats, 86–87, 536–537**
 - instant messaging (IM), 100–101**
 - insurance, 323**
 - integrated penetration testing, 519**
 - integrity, 12–13**
 - intellectual property, 235**
 - interconnection security agreement (ISA), 490**
 - interest, conflict of, 489**
 - internal audits and assessments, 511–512**
 - internal compliance, 496–497**
 - internal monitoring, 500**
 - internal threats, 84**
 - International Organization for Standardization (ISO), 445–446, 458**
 - Internet Message Access Protocol (IMAP), 364, 365**
 - Internet of Things (IoT), 197–198, 277–278**
 - Internet Protocol Security (IPSec), 227, 230**
 - interoperability, 385**
 - intrusion detection system (IDS), 216, 218–219, 229, 354–356**
 - intrusion prevention system (IPS), 218–219, 229, 354–356**
 - inventory, data, 300, 503–504**
 - investigation support, data sources for**
 - automated reports, 421
 - dashboards, 421
 - log data, 419–421
 - packet captures, 422
 - vulnerability scans, 421
 - IOCs (indicators of compromise), 169, 312, 413**
 - IoT (Internet of Things), 197–198, 277–278**
 - IPS (intrusion prevention system), 218–219, 229, 354–355**
 - signatures, 356
 - trends in, 355–356
 - IPSec, 227, 230**
 - IPS/IDS logs, 420**
 - ISA (interconnection security agreement), 490**
 - ISACs (Information Sharing And Analysis Centers), 313–314**
 - ISO (International Organization for Standardization), 445–446, 458**
 - isolation, 165**
 - ITAM. See data asset management**
-
- ## J
-
- jailbreaking, 127**
 - journaling, 261**
 - jump servers, 216–217, 229**
 - just-in-time permissions, 398**
-
- ## K
-
- key risk indicators (KRIs), 468, 473**
 - keys, security, 393–394**
 - EK (endorsement key), 56
 - key escrow, 431
 - key exchange, 50
 - key length, 50–51

- key stretching, 49–50
- keyloggers, 136
- KMS (key management system), 58
- public/private, 430–431
- SRK (storage root key), 56

KMS (key management system), 58

known penetration test environments, 520

KPIs (key performance indicators), 337, 421, 491

KRIs (key risk indicators), 468, 473

L

Layer 4/Layer 7 firewalls, 224, 230

LDAP (Lightweight Directory Access Protocol), 149, 383

least privilege, 167, 388

legacy applications, 34

legacy hardware, 121

legal hold, 414

legal implications, privacy, 504–505

legal information, 236

length of passwords, 395

lessons learned phase, incident response, 411

licenses, loss of, 498

lighting, 21–22

Lightweight Directory Access Protocol (LDAP), 149, 383

Linux permissions, 381

List Folder Contents permissions, 379–381

load balancing, 219, 229, 248–249

local data privacy, 504

Lockheed Martin, 88

log aggregation, 332–333

log data, 419–421

log scanning, 334

logic bombs, 136–137

logical segmentation, 190–191

loss of licenses, 498

Low vulnerabilities, 320

M

MAC (mandatory access control), 386–387

MAC (Media Access Control) filtering, 221, 280

machine/computer certificates, 75

maintenance phase, SDLC (software development lifecycle) policy, 442

maintenance windows, 30

malicious attacks

- application attacks, 139–147
 - buffer overflow, 149–150
 - directory traversal, 152–153
 - forgery, 151–152
 - injection, 148–149
 - privilege escalation, 150
 - replay attacks, 150
- malware attacks, 132–137
 - boatware, 135
 - keyloggers, 136
 - logic bombs, 136–137
 - ransomware, 133
 - rootkits, 137
 - spyware, 134–135
 - Trojans, 133–134
 - viruses, 136
 - worms, 134

network attacks, 139–148

- credential replay, 147
- DDoS (distributed denial-of-service), 140–142
- DNS (Domain Name System) attacks, 142–144
- malicious code, 148
- on-path, 147
- wireless, 144–147

physical attacks, 138–139

- brute-force attacks, 138
- environmental attacks, 139
- RFID (radio-frequency identification), 138

malicious code, 148

malicious updates, 117

malware, 132–137

- boatware, 135
- filtering, 369
- keyloggers, 136
- logic bombs, 136–137
- ransomware, 133
- rootkits, 137
- spyware, 134–135
- Trojans, 133–134
- viruses, 136
- worms, 134

managed service provider (MSP), 106**management attestation, 511****managerial controls, 4****mandatory access control (MAC), 386–387****Mandiant Threat Intelligence, 313****maps, threat, 312****masking, 242****master service agreements (MSAs), 489****MDM (mobile device management), 282****mean time between failures (MTBF), 479–481****mean time to failure (MTTF), 466, 479–480****mean time to repair (MTTR), 466, 479–480****measurement of security awareness programs, 547****media, removable, 538–539****Media Access Control (MAC) filtering, 221, 280****Medium vulnerabilities, 320****memorandum of agreement (MOA), 490****memorandum of understanding (MOU), 490****memory injection, 116****message-based threat vectors**

- email, 99–100
- IM (instant messaging), 100–101
- SMS (Short Message Service), 100

metadata logs, 421**MFA (multifactor authentication), 388–398****microservices, 188–189****Microsoft Azure, 185****Microsoft SCT (Security Compliance Toolkit), 269****microwave sensors, 22****MIME (Multipurpose Internet Mail Extensions), 367****misconfiguration vulnerabilities, 126****misinformation, 108–109****mitigation. *See also* access control**

- application allow lists, 164
- configuration enforcement, 167–168
- encryption, 166
- hardening techniques
 - default password changes, 173
 - definition of, 168
 - encryption, 168–169
 - endpoint protection, 169
 - HIPS (host-based intrusion prevention system), 170
 - host-based firewalls, 170
 - ports/protocols, disabling, 171–172
 - removal of unnecessary software, 173–174
- isolation, 165
- least privilege, 167
- monitoring, 167
- patching, 165–166
- risk, 476
- segmentation, 162

MITRE, 312, 320**MOA (memorandum of agreement), 490****mobile devices**

- MDM (mobile device management), 282
- securing, 270–271, 281
- vulnerabilities, 127

Modify permissions, 379–381**monitoring, 167, 291, 299**

- activities for, 332–336
 - alert response and remediation/validation, 335
 - alert tuning, 336

- alerting, 333
- archiving, 334–335
- log aggregation, 332–333
- quarantine, 335
- reporting, 334
- scanning, 334
- applications, 330–331
- definition of, 330
- infrastructure, 331–332
- internal/external, 500
- package, 311
- security awareness, 542–545
- security compliance, 499–501
- in security governance, 432–433
- systems, 330
- tools for, 336–344
 - agents/agentless, 337
 - antivirus, 341
 - benchmarks, 337
 - DLP (data loss prevention), 341–342
 - NetFlow, 343
 - SCAP (Security Content Automation Protocol), 336
 - SIEM (security information and event management) systems, 331–332, 338–340
 - SNMP (Simple Network Management Protocol), 342–343
 - vulnerability scanners, 344
 - vendors, 491–492
- MOU (memorandum of understanding), 490**
- MSAs (master service agreements), 489**
- MS-ISAC (Multi-State Information Sharing and Analysis Center), 313–314**
- MSP (managed service provider), 106**
- MTBF (mean time between failures), 479–481**
- MTTF (mean time to failure), 466, 479–480**
- MTTR (mean time to repair), 466, 479–480**
- multicloud systems, 252**

- multifactor authentication (MFA), 388–398**
- Multipurpose Internet Mail Extensions (MIME), 367**
- Multi-State Information Sharing and Analysis Center (MS-ISAC), 313–314**

N

- NAC (network access control), 371–372**
- national data privacy, 504**
- National Electrical Manufacturers Association (NEMA), 20**
- National Institute of Standards and Technology. See NIST (National Institute of Standards and Technology)**
- National Vulnerability Database (NVD), 311**
- nation-state threat actors, 88**
- NDAs (non-disclosure agreements), 235, 489**
- near-field communication (NFC), 146–147**
- needs, identifying, 545**
- negatives, false, 317**
- NEMA (National Electrical Manufacturers Association), 20**
- NetFlow, 343**
- network access control (NAC), 371–372**
- network appliances**
 - definition of, 216
 - IDS (intrusion detection system), 218–219, 229
 - IPS (intrusion prevention system), 218–219, 229
 - jump servers, 216–217, 229
 - load balancers, 219, 229
 - proxy servers, 217–218, 229
 - sensors, 220, 229
- network attacks, 139–148**
 - credential replay, 147
 - DDoS (distributed denial-of-service), 140–142
 - DNS (Domain Name System) attacks, 142–144

network attacks

- malicious code, 148
- on-path, 147
- wireless, 144–147
 - Bluetooth, 146
 - NFC (near-field communication), 146–147
 - Wi-Fi, 144–146

network infrastructure

- availability, 202
- centralized versus decentralized, 192–193
- compute resources, 207
- containerization, 193–195
- cost, 203
- definition of, 189
- ease of deployment, 204
- ease of recovery, 205
- embedded systems, 200–201
- ICS (Industrial Control Systems), 198–199
- IoT (Internet of Things), 197–198
- logical segmentation, 190–191
- patching, 205–206
- physical isolation, 189–190
- power availability, 206–207
- on-premises infrastructure, 192
- resilience, 202–203
- responsiveness, 203
- risk transference, 205
- RTOS (Real-Time Operating System), 200
- SDN (software-defined networking), 191–192
- segmentation, 162
- unsecured, 104
- virtualization, 195–197

network logs, 420–421**network scanning, 334****neutral risk appetite, 474****next-generation firewalls (NGFWs), 223–224, 230****NFC (near-field communication), 146–147****NGFWs (next-generation firewalls), 223–224, 230****NIST (National Institute of Standards and Technology), 15, 382, 427, 445–446, 456, 459****noncompliance, consequences of, 497–498****non-disclosure agreements (NDAs), 235, 489****non-human-readable data, 236–237****nonregulatory requirements, 455–458****non-repudiation, 13****NVD (National Vulnerability Database), 311****O****obfuscation, data, 242**

- data masking, 60–61
- hashing, 63–64
- overview of, 59–62
- redaction, 61
- salting, 63–64
- steganography, 62–63
- tokenization, 60

Occupational Safety and Health Administration (OSHA), 20**OCSP (Online Certificate Status Protocol), 77–78****OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 460****offboarding, 448–450****offensive penetration testing, 518****offsite backups, 257****one-time passwords (OTPs), 392****one-time risk assessments, 467–468****ongoing analysis, 544****Online Certificate Status Protocol (OCSP), 77–78****on-path network attacks, 147****on-premises infrastructure, 192****onsite backups, 257****Open Authorization (OAuth), 383–384****open public ledger, 67****open service ports, 104–105**

- Open Web Application Security Project (OWASP), 331**
- open-source intelligence (OSINT), 311–313**
- operating system security, 361–363, 420**
- operating system-based vulnerabilities, 118–119**
- operational controls, 4**
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 460**
- Opportunistic Wireless Encryption (OWE), 286**
- orchestration**
 - benefits of, 405–406
 - considerations for, 406–407
 - use cases of, 402–405
- organizational impact, 321**
- organizational validation (OV), 73–74**
- organized crime, 87–88**
- Organized Crime Control Act of 1970, 87–88**
- OSHA (Occupational Safety and Health Administration), 20**
- OSINT (open-source intelligence), 311–313**
- Others (Linux entity), 381**
- OTP (one-time password), 392**
- OV (organizational validation), 73–74**
- overflow, buffer, 149–150**
- overwriting, 301**
- OWASP (Open Web Application Security Project), 331**
- OWE (Opportunistic Wireless Encryption), 286**
- owners, 381, 473**
- ownership, 29, 297, 460, 502**

P

- P7B (PKCS#7), 76**
- PaaS (platform as a service), 182**
- package monitoring, 311**
- packet captures, 422**
- parallel processing, 255**
- partitions, 44**
- passive devices, 216, 229**
- passive reconnaissance, 516–517**
- password attacks, 154–156**
- passwordless authentication, 397**
- passwords**
 - age of, 396–397
 - complexity of, 395–396
 - default password changes, 173
 - expiration of, 396
 - length of, 395
 - management of, 397, 537–538
 - OTP (one-time password), 392
 - password concepts, 395–397
 - password vaulting, 398
 - passwordless authentication, 397
 - privileged access management tools, 397–398
 - reuse of, 396
 - standards, 446
 - switches, 272
- patching, 165–166, 205–206, 322–323**
 - cloud infrastructure, 274
 - ICS/SCADA networks, 275
 - servers, 274
 - workstations, 271
- PCI DSS (Payment Card Industry Data Security Standard), 6, 235, 454, 455, 497**
- PEM (privacy enhanced mail), 75–76**
- penetration testing, 314–315, 487**
 - components of, 514–515
 - defensive, 519
 - environments for, 520–521
 - integrated, 519
 - offensive, 518
 - overview of, 513–516
 - phases of, 515–516
 - physical tests, 517–518
 - reconnaissance, 516–517
- people, capacity planning for, 253–254**
- periodic reviews, 544**
- permissions, 164**

permissions

- assignment of, 379–381
- restrictions on, 243

personal health information (PHI), 456–458

personal identifiable information (PII), 234, 333, 456–458, 502–503

Personal Information Protection and Electronic Documents Act (PIPEDA), 504

PFX (personal information exchange), 76

philosophical motivations of threat actors, 92–93

phishing, 107–108, 526–531

- components of, 526–528
- lessons from, 528
- recognizing, 528–530
- responding to, 530–531

physical security

- access badges, 21
- access control vestibules, 19
- bollards, 19
- fencing and gates, 20
- lighting, 21–22
- overview of, 18
- physical attacks, 138–139
- physical controls, 4
- physical isolation, 189–190
- security guards, 21
- sensors, 22–23
- signs, 20
- standards, 446
- video surveillance, 20

physical tests, 517–518

PII (personal identifiable information), 234, 333, 456–458, 502–503

ping floods, 140

pinning, 79

PIPEDA (e Personal Information Protection and Electronic Documents Act), 504

PKI (public key infrastructure), 428–429

planning phase

- penetration testing, 515

- SDLC (software development lifecycle) policy, 441

platform as a service (PaaS), 182

platform diversity, 251

poisoning, DNS (Domain Name System), 143–144

policies

- acceptable use, 433–435
- business continuity, 437–438
- certificate, 72–73
- change management, 443–444
- components of, 433
- definition of, 428
- disaster recovery, 438–440
- incident response, 440–441
- information security, 435–437
- SDLC (software development lifecycle), 441–443
- updating, 35–36

policy

- administrators, 17–18
- enforcement, 369
- enforcement points, 18
- group, 361–362
- policy engines, 17
- policy-based IDSs/IPSSs, 219
- policy-driven access control, 16–17
- user guidance and training, 534–535

political motivations of threat actors, 92–93

POP (Post Office Protocol), 364, 365, 367

ports

- commonly used, 172
- disabling, 171–172
- dynamic/private, 171
- firewalls, 353
- open, 104–105
- registered, 171
- scanning, 334
- security, 220–222, 229
- selection, 365
- well-known, 171

positives, false, 317

Post Office Protocol (POP), 364, 365, 367
power availability, 206–207
power redundancy, 261–262
power supply units (PSUs), 261
praying password attacks, 155–156
preparation phase, incident response, 410

preservation, 415

pre-shared key (PSK), 288–289

pressure sensors, 22

pretexting, 109

principles of secure design

- attack surfaces, 214, 229
- connectivity, 214, 229
- device attributes, 215–216
- failure modes, 214–215, 229
- network appliances
 - definition of, 216
 - IDS (intrusion detection system), 218–219, 229
 - IPS (intrusion prevention system), 218–219, 229
- jump servers, 216–217, 229
- load balancers, 219, 229
- proxy servers, 217–218, 229
- sensors, 220, 229
- security zones, 213, 228

prioritization

- CVSS (Common Vulnerability Scoring System), 318–322
- vulnerability management, 317–318

privacy compliance

- data inventory and retention, 503–504
- definition of, 501
- legal implications of, 504–505
- privacy data roles, 501–503
- right to be forgotten, 505

privacy enhanced mail (PEM), 75–76

private data, 238, 298

private keys, 430–431

privilege escalation, 150

privileged access management tools, 397–398

procedures, 429, 447–452

procedures, updating, 35–36

process audits, 316

processors, data, 460, 503

procurement process, 296

propaganda, 108–109

proprietary data, 298

proprietary/third-party threat feeds, 313

protocol implementation, 363–366

protocols

- disabling, 171–172
- firewalls, 353
- port selection, 172, 365
- protocol selection, 364
- transport method, 365–366

provisioning, 378–379, 402

proxies, 217–218, 229, 359–360

PSK (pre-shared key), 288–289

public data, 237, 298

public key infrastructure (PKI), 428–429

public keys, 430–431

Q

qualitative risk analysis, 469–470

quantitative risk analysis, 470

quarantine, 335

questionnaires, 487

R

race conditions, 117

radio-frequency identification (RFID), 19, 138

RADIUS (Remote Authentication Dial-In User Service), 286–287

ransomware, 133

rate of return on investment (RROI), 469

RBAC (role-based access control), 387

RCA (root cause analysis), 412–413

Read & Execute permissions, 379–381

Read permissions, 381

Real-Time Operating System (RTOS), 200, 277**reconnaissance, 516–517****recovery, 411**

backups, 255–258

definition of, 255–256

differential, 256

frequency of, 258

full, 256

incremental, 256

onsite/offsite, 257

capacity planning, 253–254

COOP (continuity of operations plan), 252–253

ease of, 205

encryption, 258–259

goals of, 260

high availability, 248–249

journaling, 261

multicloud systems, 252

platform diversity, 251

power redundancy, 261–262

site considerations, 249–251

snapshots, 259

testing, 254–255

recovery point objective (RPO), 253, 467, 479**recovery time objective (RTO), 253, 467, 479****recurring reporting and monitoring, 544****recurring risk assessments, 468****redaction, 61****reflected DDoS attacks, 141–142****regional data privacy, 504****registered ports, 171****registers, risk, 472–474****regulated data, 234–235****regulatory audits, 512–513****regulatory requirements, 455–458****remediation, vulnerability, 322–325****remote access, 225–226****remote access Trojan (RAT), 134****Remote Authentication Dial-In User Service (RADIUS), 286–287****remote wipe, 271****remote work environments, 541–542****removable devices, 102, 538–539****replay attacks, 150****reporting, 326, 334, 414–415**

automated, 421

compliance, 496–497

penetration testing, 516

risk, 477–480

BIA (business impact analysis), 478–479

components of, 477–478

MTBF (mean time between failures), 479–481

MTTF (mean time to failure), 466, 479–480

MTTR (mean time to repair), 466, 479–480

RPO (recovery point objective), 479

RTO (recovery time objective), 479

security awareness, 542–545

repositories, 313**rescanning, 325–326****resilience and recovery, 202–203**

backups, 255–258

definition of, 255–256

differential, 256

frequency of, 258

full, 256

incremental, 256

onsite/offsite, 257

capacity planning, 253–254

COOP (continuity of operations plan), 252–253

encryption, 258–259

goals of, 260

high availability, 248–249

journaling, 261

multicloud systems, 252

platform diversity, 251

power redundancy, 261–262

site considerations, 249–251

- snapshots, 259
- testing, 254–255
- resource monitoring, 207. See also resource security**
- activities for, 332–336
 - alert response and remediation/validation, 335
 - alert tuning, 336
 - alerting, 333
 - archiving, 334–335
 - log aggregation, 332–333
 - quarantine, 335
 - reporting, 334
 - scanning, 334
- applications, 330–331
- definition of, 330
- infrastructure, 331–332
- systems, 330
- tools for, 336–344
 - agents/agentless, 337
 - antivirus, 341
 - benchmarks, 337
 - DLP (data loss prevention), 341–342
 - NetFlow, 343
 - SCAP (Security Content Automation Protocol), 336
 - SIEM (security information and event management) systems, 331–332, 338–340
 - SNMP (Simple Network Management Protocol), 342–343
 - vulnerability scanners, 344
- resource provisioning, 402**
- resource reuse, 122**
- resource security**
 - application security, 289–290
 - baselines, 268–269
 - cloud infrastructure, 273–274
 - connection methods, 283–285
 - deployment models, 282–283
 - embedded systems, 276
 - ICS (Industrial Control Systems), 275
 - IoT (Internet of Things), 277–278
 - MDM (mobile device management), 282
 - mobile devices, 270–271, 281
 - routers, 273
 - RTOS (Real-Time Operating System), 277
 - sandboxing, 290–291
 - SCADA (Supervisory Control and Data Acquisition), 275
 - servers, 274–275
 - switches, 272–273
 - target hardening, 270
 - wireless devices, 278–280
 - wireless security settings, 285–289
 - workstations, 271–272
- responsibilities**
 - responsibility matrix, 181–183
 - roles and, 460–462
- responsible disclosure programs, 316**
- responsiveness, network infrastructure, 203**
- restart, application, 33**
- restricted activities, 32**
- restricted data, 238**
- retention, data, 503–504**
- retina biometrics, 390**
- return on investment (ROI), 469**
- reuse of passwords, 396**
- revenge, threat actors motivated by, 93**
- reverse proxy servers, 218**
- reviews, periodic, 544**
- revision, in security governance, 432–433**
- revocation of certificates, 77**
- RFID (radio-frequency identification), 19, 138**
- right to be forgotten, 505**
- right-to-audit clause, 488**
- risk acceptance, 476**
- risk analysis, 468–472**
 - ALE (annual loss expectancy), 472
 - ARO (annual rate of occurrence), 471–472

risk analysis

qualitative, 469–470

quantitative, 470

SLE (single loss expectancy),
470–471

steps for, 468–469

risk management

acceptance, 476

analysis, 468–472

ALE (annual loss expectancy), 472

ARO (annual rate of occurrence),
471–472

qualitative, 469–470

quantitative, 470

SLE (single loss expectancy),
470–471

steps for, 468–469

assessment, 466–468

avoidance, 475–476

identification, 466

KRIs (key risk indicators), 468, 473

levels of risk, 469

mitigation, 476

reporting, 477–480

BIA (business impact analysis),
478–479

components of, 477–478

MTBF (mean time between
failures), 479–481

MTTF (mean time to failure), 466,
479–480

MTTR (mean time to repair), 466,
479–480

RPO (recovery point objective), 479

RTO (recovery time objective), 479

risk appetite, 474–475

risk identification, 466

risk owners, 473

risk registers, 472–474

risk thresholds, 473–474

risky behavior, recognizing, 532

strategies for, 475–477

third-party

agreement types, 489–491

overview of, 486

rules of engagement, 492–493

vendor assessment, 486–488

vendor monitoring, 491–492

vendor selection, 488–489

tolerance, 322, 474–475

transference of risk, 205, 476

risk owners, 473**risk registers, 472–474****risk reporting, 477–480**

BIA (business impact analysis), 478–479

components of, 477–478

MTBF (mean time between failures),
479–481

MTTF (mean time to failure), 466,
479–480

MTTR (mean time to repair), 466,
479–480

RPO (recovery point objective), 479

RTO (recovery time objective), 479

risk thresholds, 473–474**risk tolerance, 322, 474–475****risk transference, 205, 476****ROI (return on investment), 469****roles**

privacy, 501–503

RBAC (role-based access control), 387

responsibilities, 460–462

root cause analysis (RCA), 412–413**root signing certificates, 74–75****rootkits, 137****routers, 273****routine audits, 544****RPO (recovery point objective), 253, 467,
479****RROI (rate of return on investment), 469****RSA Security, 88****RTO (recovery time objective), 253, 467,
479****RTOS (Real-Time Operating System),
200, 277****rules**

block, 360–361

of engagement, 492–493

firewalls, 350–351

rule-based access control, 387

S

-
- SAE (Simultaneous Authentication of Equals), 286**
 - salting, 63–64
 - SAML (Security Assertion Markup Language), 384–385**
 - SAN certificates, 74**
 - sanctions, 498
 - sandboxing, 290–291
 - sanitization, 301–302
 - Sarbanes-Oxley Act (SOX), 235, 455**
 - SASE (Secure Access Service Edge), 228, 230**
 - SCADA (Supervisory Control and Data Acquisition), 198–199, 275, 459**
 - scanning, 334
 - rescanning, 325–326
 - URL scanning, 360
 - vulnerability scans, 308–309, 421
 - SCAP (Security Content Automation Protocol), 336**
 - scheduled reports, 544**
 - Schneier, Bruce, 476–477**
 - screened subnets, 353–354**
 - scripting**
 - benefits of, 405–406
 - considerations for, 406–407
 - use cases of, 402–405
 - SCT (Security Compliance Toolkit), 269**
 - SDLC (software development lifecycle) policy, 441–443**
 - SDN (software-defined networking), 191–192**
 - SD-WAN (software-defined wide area network), 227–228, 230**
 - sealed storage, 56
 - secret data, 298
 - Secure Access Service Edge (SASE), 228, 230**
 - Secure API, 366**
 - secure communication/access, 224–225**
 - secure cookies, 290**
 - secure enclave, 58**
 - Secure FTP (FTPS/SFTP), 366**
 - secure protocol implementation, 363–366**
 - port selection, 365
 - protocol selection, 364
 - transport method, 365–366
 - Secure Shell (SSH), 272**
 - Secure Sockets Layer (SSL), 48, 67, 366**
 - secure web gateway (SWG), 228**
 - secured zones, 17**
 - Secure/Multipurpose Internet Mail Extensions (S/MIME), 74, 367**
 - SecurID token, 391**
 - securing resources**
 - application security, 289–290
 - baselines, 268–269
 - cloud infrastructure, 273–274
 - connection methods, 283–285
 - deployment models, 282–283
 - embedded systems, 276
 - ICS (Industrial Control Systems), 275
 - IoT (Internet of Things), 277–278
 - MDM (mobile device management), 282
 - mobile devices, 270–271
 - mobile solutions, 281
 - monitoring, 291
 - routers, 273
 - RTOS (Real-Time Operating System), 277
 - sandboxing, 290–291
 - SCADA (Supervisory Control and Data Acquisition), 275
 - servers, 274–275
 - switches, 272–273
 - target hardening, 270
 - wireless devices, 278–280
 - wireless security settings, 285–289
 - workstations, 271–272
 - security architecture**
 - cloud
 - definition of, 180–181
 - hybrid considerations, 184–185
 - responsibility matrix, 181–183

security architecture

- third-party vendors, 185–186
- data protection
 - data classifications, 237–238
 - data security methods, 240–243
 - data sovereignty, 239–240
 - data states, 239
 - data types, 234–237
 - geolocation, 240
- enterprise architecture security principles
 - attack surfaces, 214, 229
 - connectivity, 214, 229
 - device attributes, 215–216
 - failure modes, 214–215, 229
 - firewalls, 222–224, 229, 350–353
 - infrastructure considerations, 212
 - network appliances, 216–220
 - port security, 220–222, 229
 - remote access, 225–226
 - SASE (Secure Access Service Edge), 228
 - SD-WAN (software-defined wide area network), 227–228, 230
 - security zones, 213, 229
 - selection of effective controls, 228–230
 - tunneling, 226–227
 - VPNs (virtual private networks), 225
- IaC (Infrastructure as code), 186–187
- microservices, 188–189
- network infrastructure, 191–192
 - definition of, 189
 - logical segmentation, 190–191
 - physical isolation, 189–190
 - SDN (software-defined networking), 191–192
- resilience and recovery
 - backups, 255–258
 - capacity planning, 253–254
 - COOP (continuity of operations plan), 252–253
 - encryption, 258–259
 - goals of, 260
 - high availability, 248–249

- journaling, 261
- multicloud systems, 252
- platform diversity, 251
- power redundancy, 261–262
- site considerations, 249–251
- snapshots, 259
- testing, 254–255
- serverless, 187–188

Security Assertion Markup Language (SAML), 384–385**security awareness**

- anomalous behavior recognition, 532–533
- development and execution, 545–547
- overview of, 526
- phishing campaigns, 526–531
 - components of, 526–528
 - lessons from, 528
 - recognizing, 528–530
 - responding to, 530–531
- reporting and monitoring, 542–545
- user guidance and training, 533–542
 - hybrid/remote work environments, 541–542
 - insider threats, 536–537
 - operational security (OpSec), 540–541
 - password management, 537–538
 - policy and handbooks, 534–535
 - removable media and cables, 538–539
 - situational awareness, 535–536
 - social engineering, 539–540
 - steps for, 533–534

security compliance

- consequences of noncompliance, 497–498
- internal/external, 496–497
- monitoring, 499–501
- overview of, 496
- privacy compliance
 - data inventory and retention, 503–504
 - definition of, 501
 - legal implications of, 504–505

- privacy data roles, 501–503
 - right to be forgotten, 505
 - reporting, 496–497
- Security Compliance Toolkit (SCT), 269**
- Security Content Automation Protocol (SCAP), 336**
- security controls**
 - bypassing, 315, 514
 - compensating, 6–7, 324
 - corrective, 6
 - deterrent, 5
 - directive, 7
 - managerial, 4
 - nature of, 3–4
 - operational, 4
 - physical, 4
 - preventative, 5
 - technical, 4
- security governance**
 - external considerations, 453–455
 - governance structures, 430–431
 - governing framework, 428–429
 - guidelines, 428, 452–453
 - industry-specific framework, 458–460
 - monitoring, 432–433
 - policies. *See* policies
 - procedures, 429, 447–452
 - regulatory and nonregulatory requirements, 455–458
 - revision, 432–433
 - roles and responsibilities, 460–462
 - standards, 428
 - standards documents, 445–447
- security groups, 403**
- security information and event management (SIEM) systems, 216, 331–332, 338–340, 543**
- security keys, 393–394**
 - EK (endorsement key), 56
 - public/private, 430–431
 - SRK (storage root key), 56
- security logs, 333**
- security operations**
 - automation and orchestration
 - benefits of, 405–406
 - considerations for, 406–407
 - use cases of, 402–405
 - data asset management
 - acquisition/ procurement process, 296
 - assignment/accounting, 297
 - certification, 302
 - classification, 297–299
 - data retention, 303
 - destruction, 302
 - disposal/decommissioning, 300–301
 - enumeration, 300
 - inventory, 300
 - monitoring/asset tracking, 299
 - ownership, 297
 - sanitization, 301–302
 - enterprise security capabilities
 - DLP (data loss prevention), 370–371
 - DNS filtering, 366
 - EDR (endpoint detection and response), 372–373
 - email security, 367–369
 - FIM (File Integrity Monitoring), 369–370
 - firewalls, 350–353
 - IDS/IPS, 354–356
 - NAC (network access control), 371–372
 - operating system security, 361–363
 - screened subnets, 353–354
 - secure protocol implementation, 363–366
 - UBA (user behavior analytics), 373
 - web filters, 357–361
 - XDR (extended detection and response), 372–373
 - identity and access management
 - access controls, 386–388
 - attestation, 385–386
 - factors, 394–395
 - identity proofing, 381–382
 - implementations, 389–394
 - interoperability, 385

security operations

- MFA (multifactor authentication), 388–398
- password concepts, 395–397
- password managers, 397
- passwordless authentication, 397
- permissions assignment, 379–381
- privileged access management tools, 397–398
- provisioning/de-provisioning user accounts, 378–379
- SSO (single sign-on), 382–385
- incident response
 - digital forensics, 414–415
 - process for, 410–411
 - RCA (root cause analysis), 412–413
 - threat hunting, 413
 - training and testing, 411–412
- monitoring
 - activities for, 332–336
 - applications, 330–331
 - definition of, 330
 - infrastructure, 331–332
 - systems, 330
- resource monitoring, 336–344
- securing resources
 - application security, 289–290
 - baselines, 268–269
 - cloud infrastructure, 273–274
 - connection methods, 283–285
 - deployment models, 282–283
 - embedded systems, 276
 - ICS (Industrial Control Systems), 275
 - IoT (Internet of Things), 277–278
 - MDM (mobile device management), 282
 - mobile devices, 270–271
 - mobile solutions, 281
 - monitoring, 291
 - routers, 273
 - RTOS (Real-Time Operating System), 277
 - sandboxing, 290–291
 - SCADA (Supervisory Control and Data Acquisition), 275
 - servers, 274–275
 - switches, 272–273
 - target hardening, 270
 - wireless devices, 278–280
 - wireless security settings, 285–289
 - workstations, 271–272
- security operations, business processes impacting, 28–31**
- security program management. *See also* risk management**
 - audits and assessments
 - attestation, 510–511
 - external, 512–513
 - internal, 511–512
 - overview of, 510
 - penetration testing, 513–521
 - security awareness
 - anomalous behavior recognition, 532–533
 - development and execution, 545–547
 - overview of, 526
 - phishing campaigns, 526–531
 - reporting and monitoring, 542–545
 - user guidance and training, 533–542
 - security compliance
 - consequences of noncompliance, 497–498
 - monitoring, 499–501
 - overview of, 496
 - privacy compliance, 501–505
 - reporting, 496–497
 - security governance
 - external considerations, 453–455
 - governance structures, 430–431
 - governing framework, 428–429
 - guidelines, 428, 452–453
 - industry-specific framework, 458–460
 - monitoring, 432–433
 - policies. *See* policies
 - procedures, 429, 447–452

- regulatory and nonregulatory requirements, 455–458
- revision, 432–433
- roles and responsibilities, 460–462
- standards, 428
- standards documents, 445–447
- third-party risk management
 - agreement types, 489–491
 - overview of, 486
 - rules of engagement, 492–493
 - vendor assessment, 486–488
 - vendor monitoring, 491–492
 - vendor selection, 488–489
- vulnerability management
 - analysis, 316–317
 - application security, 309–311
 - audits, 326
 - confirmation, 317
 - CVSS (Common Vulnerability Scoring System), 318–322
 - identification methods, 308
 - penetration testing, 314–315
 - prioritization, 317–318
 - reporting, 326
 - rescanning, 325–326
 - responsible disclosure programs, 316
 - system or process audits, 316
 - threat feeds, 311–314
 - verification, 326
 - vulnerability response and remediation, 322–325
 - vulnerability scans, 308–309
- security zones, 213, 228**
- SED (self-encrypting drive), 46**
- segmentation, 162, 190–191, 243, 324**
- self-assessments, 512**
- self-encrypting drive (SED), 46**
- self-signed certificates, 74**
- SELinux, 363**
- Sender Policy Framework (SPF), 368**
- sensitive data, 238, 298**
- sensors, 22–23, 220, 229**
- serverless architecture, 187–188**
- servers**
 - jump, 216–217, 229
 - proxy, 217–218, 229
 - securing, 274–275
- service disruptions, threat actors motivated by, 91–92**
- service level agreements (SLAs), 489–490**
- Service Organizational Control (SOC), 458**
- service packs, 323**
- service providers, 124**
- service restart, 33**
- service set identifier (SSID), 280**
- services, enabling/disabling, 404**
- shadow IT, 89**
- Short Message Service (SMS), 100**
- side loading, 127**
- SIEM (security information and event management) systems, 216, 331–332, 338–340, 543**
- signature biometrics, 390**
- signature-based IDSs/IPSs, 218, 356**
- signatures, digital, 64–66, 241**
- signs, 20**
- Simple Mail Transfer Protocol (SMTP), 364, 365**
- Simple Network Management Protocol (SNMP), 342–343, 364, 365**
- simulations, 255, 412**
- Simultaneous Authentication of Equals (SAE), 286**
- single loss expectancy (SLE), 470–471**
- single point of failure, 407**
- single sign-on (SSO), 382–385**
- site considerations, resilience and recovery, 249–251**
- site surveys, 278**
- situational awareness, 535–536**
- SLAs (service level agreements), 489–490**
- SLE (single loss expectancy), 470–471**

SLTT (State, Local, Tribal, and Territorial) government sectors

- SLTT (State, Local, Tribal, and Territorial) government sectors**, 313–314
- S/MIME (Secure/Multipurpose Internet Mail Extensions)**, 74, 367
- smishing, 108
- SMS (Short Message Service)**, 100, 108
- SMTP (Simple Mail Transfer Protocol)**, 364, 365
- smurfing, 140
- snapshots, 259
- SNMP (Simple Network Management Protocol)**, 342–343, 364, 365
- snooping, **DHCP (Dynamic Host Configuration Protocol)**, 221
- Snowden, Edward, 87
- SOC (Service Organizational Control)**, 458
- social engineering, 106–112, 539–540
- Society for Worldwide Interbank Financial Telecommunication (SWIFT)**, 454
- soft authentication tokens, 391–393
- software as a service (SaaS), 182
- software development lifecycle (SDLC) policy, 441–443
- software providers, 125
- software updates. *See* updates
- software-defined networking (SDN), 191–192
- software-defined wide area network (SD-WAN), 227–228, 230
- sophistication of threat actors, 84
- SOPs (standard operating procedures)**, 31
- sovereignty, data, 239–240
- SOW (statement of work)**, 490
- SOX (Sarbanes-Oxley Act)**, 235, 455
- spam filtering, 369
- SPF (Sender Policy Framework)**, 368
- spyware, 134–135
- SQL injection**, 120, 149
- SRK (storage root key)**, 56
- SSH (Secure Shell)**, 272
- SSID (service set identifier)**, 280
- SSL (Secure Sockets Layer)**, 48, 67, 366
- SSO (single sign-on)**, 382–385
- stakeholders, 29
- standard operating procedures (SOPs), 31
- standards, 428, 445–447
- stapling, **OCSP**, 78
- State, Local, Tribal, and Territorial (SLTT) government sectors, 313–314
- stateful protocol analysis, 219
- statement of work (SOW), 490
- states, data, 239
- static analysis, 290, 310
- steganography, 62–63, 242
- stewards, 460–461
- STIX (Structured Threat Information eXpression)**, 312
- storage root key (SRK), 56
- strategies, risk management, 475–477
- stream ciphers, 52
- stretching, key, 49–50
- Structured Threat Information eXpression (STIX)**, 312
- subjects, 17, 502
- subnets, screened, 353–354
- Supervisory Control and Data Acquisition (SCADA)**, 198–199, 275, 459
- supply chain, 105–106, 123–125, 488, 492
- supportability, 407
- surveillance, video, 20
- SWG (secure web gateway)**, 228
- SWIFT (Society for Worldwide Interbank Financial Telecommunication)**, 454
- switches, securing, 272–273
- symmetric algorithms, 51–53
- SYN floods**, 141
- synchronous replication, 260
- systems, 17
 - monitoring, 330
 - roles and responsibilities, 460–462
 - system event logs, 332
 - system or process audits, 316
 - unsupported, 103–104

T

table-top exercises, 412

tabletop exercises, 254–255

tap/monitor devices, 216, 229

target hardening, 270

TAXII (Trusted Automated eXchange of Indicator Information), 312

TBS (TPM Base Services), 57

TCG (Trusted Computing Group), 46

technical controls, 4

technical debt, 407

tehnology, capacity planning for, 254

Telnet, 364

test results, 30

testing

continuous integration and testing,
404–405

failover, 255

incident response, 411–412

parallel processing, 255

penetration, 314–315, 487

components of, 514–515

defensive, 519

environments for, 520–521

integrated, 519

offensive, 518

overview of, 513–516

phases of, 515–516

physical tests, 517–518

resilience and recovery, 254–255

SDLC (software development lifecycle)
policy, 442

security controls, 315

simulation, 255

tabletop exercises, 254–255

test results, 30

TFTP (Trivial File Transfer Protocol), 364

third-party risk management

overview of, 486

rules of engagement, 492–493

vendor assessment, 486–488

vendor monitoring, 491–492

vendor selection, 486–488

third-party threat feeds, 313

third-party vendors

cloud computing, 185–186

IaC (Infrastructure as code), 186–187

threat actors

attributes of, 84

definition of, 84

hacktivists, 87

insider threats, 86–87

motivations of, 90–94

nation-state, 88

organized crime, 87–88

shadow IT, 89

unskilled attackers, 86

threat feeds, 311–314

threat hunting, 413

threat maps, 312

threat scope reduction, 16

threat vectors, 98. See also penetration testing

default credentials, 105

definition of, 98

file-based, 101

human vectors/social engineering,
106–112

insider, 536–537

internal/external, 84

malicious attacks

application attacks, 148–153

cryptographic attacks, 153–154

indicators of, 156–157

malware attacks, 132–137

network attacks, 139–148

password attacks, 154–156

physical attacks, 138–139

message-based

email, 99–100

IM (instant messaging), 100–101

SMS (Short Message Service), 100

open service ports, 104–105

removable devices, 102

resources and funding for, 84

supply chain, 105–106

threat vectors

- unsecured networks, 104
- unsupported systems and applications, 103–104
- verifying, 315, 514
- voice calls, 101
- vulnerable software, 103
- thresholds, risk, 473–474**
- ticket creation and escalation, 403–404**
- time-based one-time password (TOTP), 392**
- time-of-check to time-of-use (TOCTOU), 117**
- time-of-day restrictions, 388**
- TLS (Transport Layer Security), 48, 226–227, 230**
- TOCTOU (time-of-check to time-of-use), 117**
- tokenization, 60, 242**
- tolerance for risk, 322, 474–475**
- top secret data, 298**
- TOTP (time-based one-time password), 392**
- TPM (Trusted Platform Module), 47, 55–57, 296**
- TPM Base Services (TBS), 57**
- trade secrets, 235**
- training. *See also* security awareness**
 - incident response, 411–412
 - user, 533–542
 - hybrid/remote work environments, 541–542
 - insider threats, 536–537
 - operational security (OpSec), 540–541
 - password management, 537–538
 - policy and handbooks, 534–535
 - removable media and cables, 538–539
 - situational awareness, 535–536
 - social engineering, 539–540
 - steps for, 533–534
- transference of risk, 205, 476**
- transit, data in, 239**
- transport encryption, 48–49**

- Transport Layer Security (TLS), 48, 67, 226–227, 230**
- transport method, 365–366**
- trends, IDS/IPS, 355–356**
- Triple DES (3DES), 166**
- Trivial File Transfer Protocol (TFTP), 364**
- Trojans, 133–134**
- trust models, 71–72**
- Trusted Automated eXchange of Indicator Information (TAXII), 312**
- Trusted Computing Group (TCG), 46**
- Trusted Platform Module (TPM), 47, 55–57, 296**
- TTPs (adversary tactics, techniques, and procedures), 312**
- tunneling, 226–227, 366**
- Twitter, 498**
- Type 1 hypervisors, 196–197**
- Type 2 hypervisors, 196–197**
- types, data, 234–237**
- typosquatting, 111–112**

U

- UBA (user behavior analytics), 373**
- UBS PaineWebber, 136–137**
- UEBA (user and entity behavior analytics) systems, 532**
- unexpected behavior, recognizing, 532**
- unified threat management (UTM), 223, 230**
- unintentional behavior, recognizing, 532**
- uninterruptible power supply (UPS), 261–262**
- Universal Resource Locator (URL) redirection, 143**
- unknown penetration test environments, 520**
- unnecessary software, removing, 173–174**
- unsecured networks, 104**
- unskilled attackers, 86**
- unsupported systems and applications, 103–104**
- updates, 271, 323**

updating

- diagrams, 35
- policies/procedures, 35–36

UPS (uninterruptible power supply), 261–262**URL (Universal Resource Locator) redirection, 143****URL scanning, 360****use, data in, 239****user accounts, provisioning/de-provisioning, 378–379****user and entity behavior analytics (UEBA) systems, 532****user attestation, 511****user behavior analytics (UBA), 373****user certificates, 75****user guidance and training, 533–542**

- hybrid/remote work environments, 541–542
- insider threats, 536–537
- operational security (OpSec), 540–541
- password management, 537–538
- policy and handbooks, 534–535
- removable media and cables, 538–539
- situational awareness, 535–536
- social engineering, 539–540
- steps for, 533–534

user provisioning, 402**UTM (unified threat management), 223, 230****V****variables, environmental, 321****vein/blood vessel biometrics, 390****vendors**

- agreement types, 489–491
- assessment of, 486–488
- monitoring, 491–492
- selection of, 488–489

version control, 36**vestibules, access control, 19****video surveillance, 20****virtual machines, 122, 259****virtual private networks (VPNs), 225, 230, 366****virtualization, 121–122, 195–197****viruses, 136****vishing, 108****VM (virtual machine) escape, 122****voice calls, as threat vectors, 101****voice phishing, 108****voiceprint, 390****VPNs (virtual private networks), 225, 230, 366****VulnDB, 312****vulnerabilities. See also penetration testing; threat vectors**

- application, 116–118
- classification of, 320
- cloud-specific, 122–123
- cryptographic, 125–126
- hardware, 120–121
- malicious attacks
 - application attacks, 148–153
 - cryptographic attacks, 153–154
 - indicators of, 156–157
 - malware attacks, 132–137
 - network attacks, 139–148
 - password attacks, 154–156
 - physical attacks, 138–139
- management of
 - analysis, 316–317
 - application security, 309–311
 - audits, 326
 - confirmation, 317
 - CVSS (Common Vulnerability Scoring System), 318–322
 - environmental variables, 321
 - exploiting vulnerabilities, 315
 - exposure factors, 321
 - identification methods, 308
 - industry/organizational impact, 321–322
 - penetration testing, 314–315
 - prioritization, 317–318
 - reporting, 326

- rescanning, 325–326
- responsible disclosure programs, 316
- risk tolerance, 322
- system or process audits, 316
- threat feeds, 311–314
- verification, 326
- vulnerability classification, 320
- vulnerability databases, 312
- vulnerability response and remediation, 322–325
- vulnerability scans, 308–309
- misconfiguration, 126
- mobile devices, 127
- operating system-based vulnerabilities, 118–119
- response and remediation, 322–325
- scanning for, 308–309, 334, 344, 421
- supply chain, 123–125
- virtualization, 121–122
- web-based, 119–120
- zero-day, 127–128

vulnerable software, 103

W

WAF (web application firewall), 222–223, 229

war, threat actors motivated by, 94

warm sites, 250

watering hole attacks, 110

web application firewall (WAF), 222–223, 229

web filters, 357–361

web-based vulnerabilities, 119–120

well-known ports, 171

WEP (Wired Equivalent Privacy), 287

Wi-Fi, 144–146, 284

- Wi-Fi Enhanced Open, 286
- WPA (Wi-Fi Protected Access), 287
- WPA2 (Wi-Fi Protected Access Version 2), 287–288
- WPA3 (Wi-Fi Protected Access Version

- 3), 285–286, 288

wildcard certificates, 74

Windows permissions, 379–381

Wired Equivalent Privacy (WEP), 287

wired networks, unsecured, 104

wireless network attacks, 144–147

- Bluetooth, 146
- NFC (near-field communication), 146–147
- unsecured networks, 104
- Wi-Fi, 144–146

wireless security, 278–280, 285–289

WO (work order), 490

work environments, hybrid/remote, 541–542

work order (WO), 490

workstations, securing, 271–272

worms, 134

WPA (Wi-Fi Protected Access), 287

WPA2 (Wi-Fi Protected Access Version 2), 287–288

WPA3 (Wi-Fi Protected Access Version 3), 285–286, 288

Write permissions, 381

X

X.509 certificates, 67–68

XACML (Extensible Access Control Markup Language), 387–388

XDR (extended detection and response), 372–373

XML injection, 149

XSS (cross-site scripting), 120, 148–149

Y-Z

Zero Trust architecture (ZTA), 15–18

Zero Trust network access (ZTNA), 228

zero-day vulnerability, 127–128

zones, security, 17, 213, 228

ZTE, 498