

“All-in-One Is All You Need.”

ALL-IN-ONE

CISSP®

EXAM GUIDE
NINTH EDITION

*Fully updated coverage
of all 8 domains for the
2021 Certified Information
Systems Security
Professional exam*

*Ideal as both a study guide
and an on-the-job reference*

*Filled with practice exam
questions and in-depth
explanations*

**Mc
Graw
Hill**

**Online content
includes:**

- 1400+ practice exam questions
- Graphical question quizzes
- Test engine that provides full-length practice exams and customizable quizzes by chapter or exam domain
- Access to Flash cards

FERNANDO MAYMÍ, PhD, CISSP
SHON HARRIS, CISSP

Praise for *CISSP® All-in-One Exam Guide*

Fernando's latest update to the *CISSP All-In-One Exam Guide* continues the tradition started in past collaborations with Shon Harris of breaking down key concepts and critical skills in a way that prepares the reader for the exam. Once again the material proves to be not only a vital asset to exam preparation but a valued resource reference for use well after the exam has been passed.

Stefanie Keuser, CISSP,
Chief Information Officer,
Military Officers Association of America

The *CISSP All-in-One Exam Guide* is the only book one needs to pass the CISSP exam. Fernando Maymí is not just an author, he is a leader in the cybersecurity industry. His insight, knowledge, and expertise is reflected in the content provided in this book. The book will not only give you what you need to pass the exam, it can also be used to help you further your career in cybersecurity.

Marc Coady, CISSP,
Compliance Analyst,
Costco Wholesale

A must-have reference for any cyber security practitioner, this book provides invaluable practical knowledge on the increasingly complex universe of security concepts, controls, and best practices necessary to do business in today's world.

Steve Zalewski,
Former Chief Information Security Officer,
Levi Strauss & Co.

Shon Harris put the CISSP certification on the map with this golden bible of the CISSP. Fernando Maymí carries that legacy forward beautifully with clarity, accuracy, and balance. I am sure that Shon would be proud.

David R. Miller, CISSP, CCSP, GIAC GISP GSEC GISE,
PCI QSA, LPT, ECSA, CEH, CWNA, CCNA, SME, MCT,
MCIT Pro EA, MCSE: Security, CNE, Security+, etc.

An excellent reference. Written clearly and concisely, this book is invaluable to students, educators, and practitioners alike.

Dr. Joe Adams,
Founder and Executive Director,
Michigan Cyber Range

A lucid, enlightening, and comprehensive tour de force through the breadth of cyber security. Maymí and Harris are masters of the craft.

Dr. Greg Conti,
Founder,
Kopidion LLC

I wish I found this book earlier in my career. It certainly was the single tool I used to pass the CISSP exam, but more importantly it has taught me about security from many aspects I did not even comprehend previously. I think the knowledge that I gained from this book is going to help me in many years to come. Terrific book and resource!

Janet Robinson,
Chief Security Officer

ALL ■ IN ■ ONE

CISSP®

EXAM GUIDE

ABOUT THE AUTHORS



Fernando Maymí, PhD, CISSP, is a security practitioner with over 25 years' experience in the field. He is currently Vice President of Training at IronNet Cybersecurity, where, besides developing cyber talent for the company, its partners, and customers, he has led teams providing strategic consultancy, security assessments, red teaming, and cybersecurity exercises around the world. Previously, he led advanced research and development projects at the intersection of artificial intelligence and cybersecurity, stood up the U.S. Army's think tank for strategic cybersecurity issues, and was a West Point faculty member for over 12 years. Fernando worked closely with Shon Harris, advising her on a multitude of projects, including the sixth edition of the *CISSP All-in-One Exam Guide*.

Shon Harris, CISSP, was the founder and CEO of Shon Harris Security LLC and Logical Security LLC, a security consultant, a former engineer in the Air Force's Information Warfare unit, an instructor, and an author. Shon owned and ran her own training and consulting companies for 13 years prior to her death in 2014. She consulted with Fortune 100 corporations and government agencies on extensive security issues. She authored three best-selling CISSP books, was a contributing author to *Gray Hat Hacking: The Ethical Hacker's Handbook* and *Security Information and Event Management (SIEM) Implementation*, and a technical editor for *Information Security Magazine*.

About the Contributor/Technical Editor

Bobby E. Rogers is an information security engineer working as a contractor for Department of Defense agencies, helping to secure, certify, and accredit their information systems. His duties include information system security engineering, risk management, and certification and accreditation efforts. He retired after 21 years in the U.S. Air Force, serving as a network security engineer and instructor, and has secured networks all over the world. Bobby has a master's degree in information assurance (IA) and is pursuing a doctoral degree in cybersecurity from Capitol Technology University in Maryland. His many certifications include CISSP-ISSEP, CEH, and MCSE: Security, as well as the CompTIA A+, Network+, Security+, and Mobility+ certifications.

ALL ■ IN ■ ONE

CISSP®

EXAM GUIDE

Ninth Edition

Fernando Maymí
Shon Harris



New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

McGraw Hill is an independent entity from (ISC)²® and is not affiliated with (ISC)² in any manner. This study/training guide and/or material is not sponsored by, endorsed by, or affiliated with (ISC)² in any manner. This publication and accompanying media may be used in assisting students to prepare for the CISSP exam. Neither (ISC)² nor McGraw Hill warrants that use of this publication and accompanying media will ensure passing any exam. (ISC)²®, CISSP®, CAP®, ISSAP®, ISSEP®, ISSMP®, SSCP® and CBK® are trademarks or registered trademarks of (ISC)² in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Copyright © 2022 by McGraw Hill. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

ISBN: 978-1-26-046736-9

MHID: 1-26-046736-8

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-046737-6,
MHID: 1-26-046737-6.

eBook conversion by codeMantra
Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information has been obtained by McGraw Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw Hill, or others, McGraw Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." MCGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

We dedicate this book to all those
who have served others selflessly.

This page intentionally left blank

CONTENTS AT A GLANCE

Part I	Security and Risk Management	
Chapter 1	Cybersecurity Governance	3
Chapter 2	Risk Management	53
Chapter 3	Compliance	125
Chapter 4	Frameworks	171
Part II	Asset Security	
Chapter 5	Assets	213
Chapter 6	Data Security	253
Part III	Security Architecture and Engineering	
Chapter 7	System Architectures	283
Chapter 8	Cryptology	317
Chapter 9	Security Architectures	385
Chapter 10	Site and Facility Security	417
Part IV	Communication and Network Security	
Chapter 11	Networking Fundamentals	469
Chapter 12	Wireless Networking	559
Chapter 13	Securing the Network	597
Chapter 14	Network Components	643
Chapter 15	Secure Communications Channels	681
Part V	Identity and Access Management	
Chapter 16	Identity and Access Fundamentals	715
Chapter 17	Managing Identities and Access	765

Part VI	Security Assessment and Testing	
Chapter 18	Security Assessments	813
Chapter 19	Measuring Security.....	851
Part VII	Security Operations	
Chapter 20	Managing Security Operations.....	885
Chapter 21	Security Operations	939
Chapter 22	Security Incidents	989
Chapter 23	Disasters.....	1029
Part VIII	Software Development Security	
Chapter 24	Software Development	1079
Chapter 25	Secure Software	1117
Appendix A	Comprehensive Questions	1155
Appendix B	Objective Map	1209
Appendix C	About the Online Content.....	1225
	Glossary	1231
	Index.....	1253

CONTENTS

From the Author	xxix
Acknowledgments	xxxiii
Why Become a CISSP?	xxxv

Part I Security and Risk Management

Chapter 1	Cybersecurity Governance	3
	Fundamental Cybersecurity Concepts and Terms	4
	Confidentiality	5
	Integrity	5
	Availability	6
	Authenticity	6
	Nonrepudiation	6
	Balanced Security	7
	Other Security Terms	8
	Security Governance Principles	10
	Aligning Security to Business Strategy	13
	Organizational Processes	17
	Organizational Roles and Responsibilities	18
	Security Policies, Standards, Procedures, and Guidelines	25
	Security Policy	27
	Standards	29
	Baselines	31
	Guidelines	32
	Procedures	32
	Implementation	32
	Personnel Security	33
	Candidate Screening and Hiring	35
	Employment Agreements and Policies	36
	Onboarding, Transfers, and Termination Processes	37
	Vendors, Consultants, and Contractors	39
	Compliance Policies	39
	Privacy Policies	40
	Security Awareness, Education, and Training Programs	40
	Degree or Certification?	40
	Methods and Techniques to Present	
	Awareness and Training	41

Periodic Content Reviews	43
Program Effectiveness Evaluation	43
Professional Ethics	44
(ISC) ² Code of Professional Ethics	44
Organizational Code of Ethics	45
The Computer Ethics Institute	45
Chapter Review	46
Quick Review	46
Questions	48
Answers	51
Chapter 2 Risk Management	53
Risk Management Concepts	53
Holistic Risk Management	54
Information Systems Risk Management Policy	56
The Risk Management Team	56
The Risk Management Process	57
Overview of Vulnerabilities and Threats	58
Identifying Threats and Vulnerabilities	62
Assessing Risks	63
Asset Valuation	65
Risk Assessment Teams	66
Methodologies for Risk Assessment	67
Risk Analysis Approaches	72
Qualitative Risk Analysis	76
Responding to Risks	79
Total Risk vs. Residual Risk	81
Countermeasure Selection and Implementation	81
Types of Controls	83
Control Assessments	88
Monitoring Risks	91
Effectiveness Monitoring	91
Change Monitoring	92
Compliance Monitoring	93
Risk Reporting	94
Continuous Improvement	95
Supply Chain Risk Management	96
Upstream and Downstream Suppliers	98
Risks Associated with Hardware, Software, and Services	98
Other Third-Party Risks	99
Minimum Security Requirements	100
Service Level Agreements	101
Business Continuity	101
Standards and Best Practices	104
Making BCM Part of the Enterprise Security Program	106
Business Impact Analysis	108

Chapter Review	116
Quick Review	116
Questions	118
Answers	121
Chapter 3 Compliance	125
Laws and Regulations	125
Types of Legal Systems	126
Common Law Revisited	129
Cybercrimes and Data Breaches	130
Complexities in Cybercrime	132
The Evolution of Attacks	134
International Issues	138
Data Breaches	139
Import/Export Controls	145
Transborder Data Flow	146
Privacy	147
Licensing and Intellectual Property Requirements	147
Trade Secret	148
Copyright	149
Trademark	150
Patent	151
Internal Protection of Intellectual Property	152
Software Piracy	153
Compliance Requirements	155
Contractual, Legal, Industry Standards, and Regulatory Requirements	156
Privacy Requirements	158
Liability and Its Ramifications	158
Requirements for Investigations	161
Administrative	161
Criminal	162
Civil	162
Regulatory	162
Chapter Review	162
Quick Review	163
Questions	165
Answers	168
Chapter 4 Frameworks	171
Overview of Frameworks	171
Risk Frameworks	173
NIST RMF	173
ISO/IEC 27005	177
OCTAVE	178
FAIR	179

Information Security Frameworks	179
Security Program Frameworks	180
Security Control Frameworks	183
Enterprise Architecture Frameworks	189
Why Do We Need Enterprise Architecture Frameworks?	191
Zachman Framework	192
The Open Group Architecture Framework	194
Military-Oriented Architecture Frameworks	195
Other Frameworks	196
ITIL	196
Six Sigma	197
Capability Maturity Model	197
Putting It All Together	199
Chapter Review	203
Quick Review	203
Questions	205
Answers	208

Part II Asset Security

Chapter 5 Assets	213
Information and Assets	214
Identification	214
Classification	215
Physical Security Considerations	220
Protecting Mobile Devices	220
Paper Records	221
Safes	221
Managing the Life Cycle of Assets	222
Ownership	223
Inventories	224
Secure Provisioning	227
Asset Retention	228
Data Life Cycle	230
Data Acquisition	230
Data Storage	232
Data Use	237
Data Sharing	238
Data Archival	239
Data Destruction	240
Data Roles	244
Chapter Review	245
Quick Review	245
Questions	247
Answers	250

Chapter 6	Data Security	253
	Data Security Controls	253
	Data States	254
	Standards	258
	Scoping and Tailoring	258
	Data Protection Methods	258
	Digital Asset Management	261
	Digital Rights Management	263
	Data Loss Prevention	265
	Cloud Access Security Broker	275
	Chapter Review	276
	Quick Review	276
	Questions	277
	Answers	279

Part III Security Architecture and Engineering

Chapter 7	System Architectures	283
	General System Architectures	283
	Client-Based Systems	284
	Server-Based Systems	284
	Database Systems	285
	High-Performance Computing Systems	288
	Industrial Control Systems	289
	Devices	291
	Distributed Control System	293
	Supervisory Control and Data Acquisition	294
	ICS Security	294
	Virtualized Systems	296
	Virtual Machines	296
	Containerization	298
	Microservices	299
	Serverless	299
	Cloud-Based Systems	301
	Software as a Service	302
	Platform as a Service	303
	Infrastructure as a Service	304
	Everything as a Service	304
	Cloud Deployment Models	305
	Pervasive Systems	305
	Embedded Systems	306
	Internet of Things	306
	Distributed Systems	307
	Edge Computing Systems	308

Chapter Review	310
Quick Review	310
Questions	311
Answers	314
Chapter 8 Cryptology	317
The History of Cryptography	317
Cryptography Definitions and Concepts	321
Cryptosystems	323
Kerckhoffs' Principle	324
The Strength of the Cryptosystem	325
One-Time Pad	325
Cryptographic Life Cycle	328
Cryptographic Methods	328
Symmetric Key Cryptography	329
Asymmetric Key Cryptography	335
Elliptic Curve Cryptography	342
Quantum Cryptography	344
Hybrid Encryption Methods	346
Integrity	351
Hashing Functions	351
Message Integrity Verification	354
Public Key Infrastructure	359
Digital Certificates	359
Certificate Authorities	360
Registration Authorities	362
PKI Steps	362
Key Management	364
Attacks Against Cryptography	367
Key and Algorithm Attacks	367
Implementation Attacks	370
Other Attacks	372
Chapter Review	375
Quick Review	376
Questions	379
Answers	381
Chapter 9 Security Architectures	385
Threat Modeling	385
Attack Trees	386
STRIDE	387
The Lockheed Martin Cyber Kill Chain	387
The MITRE ATT&CK Framework	389
Why Bother with Threat Modeling	389

Secure Design Principles	390
Defense in Depth	390
Zero Trust	392
Trust But Verify	392
Shared Responsibility	392
Separation of Duties	393
Least Privilege	394
Keep It Simple	395
Secure Defaults	396
Fail Securely	396
Privacy by Design	397
Security Models	397
Bell-LaPadula Model	398
Biba Model	399
Clark-Wilson Model	400
Noninterference Model	400
Brewer and Nash Model	402
Graham-Denning Model	402
Harrison-Ruzzo-Ullman Model	402
Security Requirements	404
Security Capabilities of Information Systems	404
Trusted Platform Module	404
Hardware Security Module	406
Self-Encrypting Drive	407
Bus Encryption	407
Secure Processing	408
Chapter Review	411
Quick Review	412
Questions	413
Answers	415
Chapter 10 Site and Facility Security	417
Site and Facility Design	417
Security Principles	418
The Site Planning Process	423
Crime Prevention Through Environmental Design	427
Designing a Physical Security Program	433
Site and Facility Controls	441
Work Area Security	441
Data Processing Facilities	443
Distribution Facilities	446
Storage Facilities	447
Utilities	448
Fire Safety	454
Environmental Issues	461

Chapter Review	461
Quick Review	461
Questions	463
Answers	465

Part IV Communication and Network Security

Chapter 11	Networking Fundamentals	469
	Data Communications Foundations	469
	Network Reference Models	470
	Protocols	471
	Application Layer	474
	Presentation Layer	475
	Session Layer	477
	Transport Layer	479
	Network Layer	480
	Data Link Layer	480
	Physical Layer	483
	Functions and Protocols in the OSI Model	483
	Tying the Layers Together	485
	Local Area Networks	487
	Network Topology	487
	Medium Access Control Mechanisms	489
	Layer 2 Protocols	494
	Transmission Methods	499
	Layer 2 Security Standards	500
	Internet Protocol Networking	502
	TCP	503
	IP Addressing	510
	IPv6	512
	Address Resolution Protocol	515
	Dynamic Host Configuration Protocol	517
	Internet Control Message Protocol	520
	Simple Network Management Protocol	522
	Domain Name Service	524
	Network Address Translation	531
	Routing Protocols	533
	Intranets and Extranets	537
	Metropolitan Area Networks	538
	Metro Ethernet	539
	Wide Area Networks	540
	Dedicated Links	541
	WAN Technologies	543

Chapter Review	552
Quick Review	553
Questions	555
Answers	557
Chapter 12 Wireless Networking	559
Wireless Communications Techniques	559
Spread Spectrum	561
Orthogonal Frequency Division Multiplexing	563
Wireless Networking Fundamentals	564
WLAN Components	564
WLAN Standards	565
Other Wireless Network Standards	568
Other Important Standards	573
Evolution of WLAN Security	574
802.11	575
802.11i	576
802.11w	578
WPA3	578
802.1X	579
Best Practices for Securing WLANs	582
Mobile Wireless Communication	582
Multiple Access Technologies	584
Generations of Mobile Wireless	585
Satellites	588
Chapter Review	590
Quick Review	590
Questions	592
Answers	594
Chapter 13 Securing the Network	597
Applying Secure Design Principles to Network Architectures	597
Secure Networking	599
Link Encryption vs. End-to-End Encryption	600
TLS	602
VPN	605
Secure Protocols	611
Web Services	611
Domain Name System	616
Electronic Mail	621
Multilayer Protocols	626
Distributed Network Protocol 3	626
Controller Area Network Bus	627
Modbus	627

Converged Protocols	627
Encapsulation	628
Fiber Channel over Ethernet	628
Internet Small Computer Systems Interface	629
Network Segmentation	629
VLANs	630
Virtual eXtensible Local Area Network	632
Software-Defined Networks	632
Software-Defined Wide Area Network	635
Chapter Review	635
Quick Review	636
Questions	638
Answers	640
Chapter 14 Network Components	643
Transmission Media	643
Types of Transmission	644
Cabling	648
Bandwidth and Throughput	654
Network Devices	655
Repeaters	655
Bridges	656
Switches	657
Routers	660
Gateways	662
Proxy Servers	663
PBXs	665
Network Access Control Devices	667
Network Diagramming	668
Operation of Hardware	670
Endpoint Security	673
Content Distribution Networks	674
Chapter Review	674
Quick Review	675
Questions	677
Answers	678
Chapter 15 Secure Communications Channels	681
Voice Communications	682
Public Switched Telephone Network	682
DSL	683
ISDN	685
Cable Modems	686
IP Telephony	687

Multimedia Collaboration	693
Meeting Applications	694
Unified Communications	695
Remote Access	696
VPN	697
Desktop Virtualization	699
Secure Shell	701
Data Communications	702
Network Sockets	703
Remote Procedure Calls	703
Virtualized Networks	704
Third-Party Connectivity	705
Chapter Review	707
Quick Review	707
Questions	709
Answers	711

Part V Identity and Access Management

Chapter 16 Identity and Access Fundamentals	715
Identification, Authentication, Authorization, and Accountability	715
Identification and Authentication	718
Knowledge-Based Authentication	720
Biometric Authentication	723
Ownership-Based Authentication	729
Credential Management	736
Password Managers	736
Password Synchronization	737
Self-Service Password Reset	737
Assisted Password Reset	738
Just-in-Time Access	738
Registration and Proofing of Identity	738
Profile Update	740
Session Management	740
Accountability	741
Identity Management	745
Directory Services	747
Directories' Role in Identity Management	748
Single Sign-On	750
Federated Identity Management	752
Federated Identity with a Third-Party Service	754
Integration Issues	754
On-Premise	755
Cloud	756
Hybrid	756

Chapter Review	756
Quick Review	757
Questions	759
Answers	762
Chapter 17 Managing Identities and Access	765
Authorization Mechanisms	765
Discretionary Access Control	766
Mandatory Access Control	768
Role-Based Access Control	771
Rule-Based Access Control	774
Attribute-Based Access Control	774
Risk-Based Access Control	775
Implementing Authentication and Authorization Systems	776
Access Control and Markup Languages	776
OAuth	782
OpenID Connect	783
Kerberos	784
Remote Access Control Technologies	789
Managing the Identity and Access Provisioning Life Cycle	795
Provisioning	796
Access Control	796
Compliance	796
Configuration Management	799
Deprovisioning	800
Controlling Physical and Logical Access	801
Information Access Control	801
System and Application Access Control	802
Access Control to Devices	802
Facilities Access Control	802
Chapter Review	804
Quick Review	804
Questions	805
Answers	808

Part VI Security Assessment and Testing

Chapter 18 Security Assessments	813
Test, Assessment, and Audit Strategies	813
Designing an Assessment	814
Validating an Assessment	815
Testing Technical Controls	817
Vulnerability Testing	817
Other Vulnerability Types	819
Penetration Testing	822
Red Teaming	827

Breach Attack Simulations	828
Log Reviews	828
Synthetic Transactions	832
Code Reviews	833
Code Testing	834
Misuse Case Testing	835
Test Coverage	837
Interface Testing	837
Compliance Checks	838
Conducting Security Audits	838
Internal Audits	840
External Audits	842
Third-Party Audits	843
Chapter Review	844
Quick Review	845
Questions	846
Answers	848
Chapter 19 Measuring Security	851
Quantifying Security	851
Security Metrics	853
Key Performance and Risk Indicators	855
Security Process Data	857
Account Management	858
Backup Verification	860
Security Training and Security Awareness Training	863
Disaster Recovery and Business Continuity	867
Reporting	869
Analyzing Results	870
Writing Technical Reports	872
Executive Summaries	873
Management Review and Approval	875
Before the Management Review	876
Reviewing Inputs	876
Management Approval	877
Chapter Review	877
Quick Review	878
Questions	879
Answers	881
Part VII Security Operations	
Chapter 20 Managing Security Operations	885
Foundational Security Operations Concepts	885
Accountability	887
Need-to-Know/Least Privilege	888

Separation of Duties and Responsibilities	888
Privileged Account Management	889
Job Rotation	889
Service Level Agreements	890
Change Management	891
Change Management Practices	891
Change Management Documentation	893
Configuration Management	893
Baselining	894
Provisioning	894
Automation	895
Resource Protection	895
System Images	896
Source Files	896
Backups	896
Vulnerability and Patch Management	900
Vulnerability Management	900
Patch Management	903
Physical Security	906
External Perimeter Security Controls	906
Facility Access Control	916
Internal Security Controls	924
Personnel Access Controls	924
Intrusion Detection Systems	925
Auditing Physical Access	929
Personnel Safety and Security	929
Travel	930
Security Training and Awareness	930
Emergency Management	931
Duress	931
Chapter Review	932
Quick Review	932
Questions	934
Answers	937
Chapter 21 Security Operations	939
The Security Operations Center	939
Elements of a Mature SOC	940
Threat Intelligence	941
Preventive and Detective Measures	944
Firewalls	945
Intrusion Detection and Prevention Systems	967
Antimalware Software	969
Sandboxing	972
Outsourced Security Services	973
Honeypots and Honeynets	974
Artificial Intelligence Tools	976

Logging and Monitoring	978
Log Management	978
Security Information and Event Management	979
Egress Monitoring	981
User and Entity Behavior Analytics	981
Continuous Monitoring	981
Chapter Review	982
Quick Review	983
Questions	984
Answers	986
Chapter 22 Security Incidents	989
Overview of Incident Management	989
Detection	995
Response	996
Mitigation	996
Reporting	997
Recovery	998
Remediation	999
Lessons Learned	999
Incident Response Planning	1000
Roles and Responsibilities	1000
Incident Classification	1002
Notifications	1003
Operational Tasks	1004
Runbooks	1006
Investigations	1006
Motive, Opportunity, and Means	1007
Computer Criminal Behavior	1008
Evidence Collection and Handling	1008
What Is Admissible in Court?	1013
Digital Forensics Tools, Tactics, and Procedures	1015
Forensic Investigation Techniques	1016
Other Investigative Techniques	1018
Forensic Artifacts	1020
Reporting and Documenting	1021
Chapter Review	1022
Quick Review	1022
Questions	1024
Answers	1026
Chapter 23 Disasters	1029
Recovery Strategies	1029
Business Process Recovery	1033
Data Backup	1034
Documentation	1041
Human Resources	1042

Recovery Site Strategies	1043
Availability	1049
Disaster Recovery Processes	1053
Response	1055
Personnel	1055
Communications	1056
Assessment	1058
Restoration	1058
Training and Awareness	1060
Lessons Learned	1061
Testing Disaster Recovery Plans	1061
Business Continuity	1065
BCP Life Cycle	1065
Information Systems Availability	1067
End-User Environment	1071
Chapter Review	1071
Quick Review	1072
Questions	1073
Answers	1075

Part VIII Software Development Security

Chapter 24 Software Development	1079
Software Development Life Cycle	1079
Project Management	1081
Requirements Gathering Phase	1082
Design Phase	1083
Development Phase	1087
Testing Phase	1089
Operations and Maintenance Phase	1091
Development Methodologies	1095
Waterfall Methodology	1095
Prototyping	1096
Incremental Methodology	1096
Spiral Methodology	1098
Rapid Application Development	1099
Agile Methodologies	1100
DevOps	1103
DevSecOps	1104
Other Methodologies	1104
Maturity Models	1106
Capability Maturity Model Integration	1107
Software Assurance Maturity Model	1109

Chapter Review	1110
Quick Review	1110
Questions	1112
Answers	1114
Chapter 25 Secure Software	1117
Programming Languages and Concepts	1118
Assemblers, Compilers, Interpreters	1120
Runtime Environments	1122
Object-Oriented Programming Concepts	1124
Cohesion and Coupling	1130
Application Programming Interfaces	1132
Software Libraries	1132
Secure Software Development	1133
Source Code Vulnerabilities	1133
Secure Coding Practices	1134
Security Controls for Software Development	1136
Development Platforms	1137
Tool Sets	1138
Application Security Testing	1139
Continuous Integration and Delivery	1140
Security Orchestration, Automation, and Response	1141
Software Configuration Management	1142
Code Repositories	1143
Software Security Assessments	1144
Risk Analysis and Mitigation	1144
Change Management	1145
Assessing the Security of Acquired Software	1145
Commercial Software	1146
Open-Source Software	1146
Third-Party Software	1147
Managed Services	1148
Chapter Review	1148
Quick Review	1148
Questions	1150
Answers	1152
Appendix A Comprehensive Questions	1155
Answers	1189
Appendix B Objective Map	1209
Appendix C About the Online Content	1225
System Requirements	1225
Your Total Seminars Training Hub Account	1225
Privacy Notice	1225

Single User License Terms and Conditions	1225
TotalTester Online	1227
Graphical Questions	1227
Online Flash Cards	1228
Single User License Terms and Conditions	1228
Technical Support	1229
Glossary	1231
Index	1253

FROM THE AUTHOR

Thank you for investing your resources in this ninth edition of the *CISSP All-in-One Exam Guide*. I am confident you'll find it helpful, not only as you prepare for the CISSP exam, but as a reference in your future professional endeavors. That was one of the overarching goals of Shon Harris when she wrote the first six editions and is something I've strived to uphold in the last three. It is not always easy, but I think you'll be pleased with how we've balanced these two requirements.

(ISC)² does a really good job of grounding the CISSP Common Body of Knowledge (CBK) in real-world applications, but (let's face it) there's always a lot of room for discussion and disagreements. There are very few topics in cybersecurity (or pretty much any other field) on which there is universal agreement. To balance the content of this book between exam preparation and the murkiness of real-world applications, we've included plenty of comments and examples drawn from our experiences.

I say "our experiences" deliberately because the voice of Shon remains vibrant, informative, and entertaining in this edition, years after her passing. I've preserved as many of her insights as possible while ensuring the content is up to date and relevant. I also strove to maintain the conversational tone that was such a hallmark of her work. The result is a book that (I hope) reads more like an essay (or even a story) than a textbook but is grounded in good pedagogy. It should be easy to read but still prepare you for the exam.

Speaking of the exam, the changes that (ISC)² made to the CBK in 2021 are not dramatic but are still significant. Each domain was tweaked in some way, and seven of the eight domains had multiple topics added (domain 1 was the exception here). These changes, coupled with the number of topics that were growing stale in the eighth edition of this book, prompted me to completely restructure this edition. I tore each domain and topic down to atomic particles and then re-engineered the entire book to integrate the new objectives, which are listed in Table 1.

Domain 2: Asset Security

- 2.4 Manage data lifecycle
 - 2.4.1 Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
 - 2.4.3 Data location
 - 2.4.4 Data maintenance
- 2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

Domain 3: Security Architecture and Engineering

(Under 3.7 Understand methods of cryptanalytic attacks)

- 3.7.1 Brute force
- 3.7.4 Frequency analysis

Table 1 CBK 2021: New Objectives (*continued*)

Domain 3: Security Architecture and Engineering

- 3.7.6 Implementation attacks
- 3.7.8 Fault injection
- 3.7.9 Timing
- 3.7.10 Man-in-the-Middle (MITM)
- 3.7.11 Pass the hash
- 3.7.12 Kerberos exploitation
- 3.7.13 Ransomware

(Under 3.9 Design site and facility security controls)

- 3.9.9 Power (e.g., redundant, backup)

Domain 4: Communication and Network Security

(Under 4.1 Assess and implement secure design principles in network architectures)

- 4.1.3 Secure protocols
- 4.1.6 Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
- 4.1.8 Cellular networks (e.g., 4G, 5G)

(Under 4.3 Implement secure communication channels according to design)

- 4.3.6 Third-party connectivity

Domain 5: Identity and Access Management (IAM)

(Under 5.1 Control physical and logical access to assets)

- 5.1.5 Applications

(Under 5.2 Manage identification and authentication of people, devices, and services)

- 5.2.8 Single Sign On (SSO)
- 5.2.9 Just-In-Time (JIT)

(Under 5.4 Implement and manage authorization mechanisms)

- 5.4.6 Risk based access control

(Under 5.5 Manage the identity and access provisioning lifecycle)

- 5.5.3 Role definition (e.g., people assigned to new roles)
- 5.5.4 Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)
- 5.6 Implement authentication systems
- 5.6.1 OpenID Connect (OIDC)/Open Authorization (OAuth)
- 5.6.2 Security Assertion Markup Language (SAML)
- 5.6.3 Kerberos
- 5.6.4 Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

Domain 6: Security Assessment and Testing

(Under 6.2 Conduct security control testing)

- 6.2.9 Breach attack simulations
- 6.2.10 Compliance checks

Table 1 CBK 2021: New Objectives

Domain 6: Security Assessment and Testing

(Under 6.3 Collect security process data (e.g., technical and administrative))

6.3.6 Disaster Recovery (DR) and Business Continuity (BC)

(Under 6.4 Analyze test output and generate report)

6.4.1 Remediation

6.4.2 Exception handling

6.4.3 Ethical disclosure

Domain 7: Security Operations

(Under 7.1 Understand and comply with investigations)

7.1.5 Artifacts (e.g., computer, network, mobile device)

(Under 7.2 Conduct logging and monitoring activities)

7.2.5 Log management

7.2.6 Threat intelligence (e.g., threat feeds, threat hunting)

7.2.7 User and Entity Behavior Analytics (UEBA)

(Under 7.7 Operate and maintain detective and preventative measures)

7.7.8 Machine learning and Artificial Intelligence (AI) based tools

(Under 7.11 Implement Disaster Recovery (DR) processes)

7.11.7 Lessons learned

Domain 8: Software Development Security

(Under 8.2 Identify and apply security controls in software development ecosystems)

8.2.1 Programming languages

8.2.2 Libraries

8.2.3 Tool sets

8.2.5 Runtime

8.2.6 Continuous Integration and Continuous Delivery (CI/CD)

8.2.7 Security Orchestration, Automation, and Response (SOAR)

8.2.10 Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

(Under 8.4 Assess security impact of acquired software)

8.4.1 Commercial-off-the-shelf (COTS)

8.4.2 Open source

8.4.3 Third-party

8.4.4 Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

(Under 8.5 Define and apply secure coding guidelines and standards)

8.5.4 Software-defined security

Table 1 CBK 2021: New Objectives (*continued*)

Note that some of these objectives were implicit in the previous (2018) version of the CBK and were therefore covered in the eighth edition of this book. The fact that they are now explicit is an indication of their increased importance both in the exam and in the real world. (Please pay particular attention to these as you prepare for the exam.) All in all, this ninth edition is significantly different (and improved) when compared to the previous one. I think you'll agree. Thank you, again, for investing in this ninth edition.

ACKNOWLEDGMENTS

I would like to thank all the people who work in the information security industry who are driven by their passion, dedication, and a true sense of doing right. These selfless professionals sacrifice their personal time to prevent, block, and respond to the relentless efforts of malicious actors around the world. We all sleep more peacefully at night because you remain at the ready.

In this ninth edition, I would also like to thank the following:

- Ronald C. Dodge, Jr., who introduced me to Shon Harris and, in so doing, started me off on one of the best adventures of my life
- Kathy Conlon, who, more than anyone else, set the conditions that led to nine editions of this book
- Carol Remicci
- David Harris
- The men and women of our armed forces, who selflessly defend our way of life

This page intentionally left blank

WHY BECOME A CISSP?

As our world changes, the need for improvements in security and technology continues to grow. Organizations around the globe are desperate to identify and recruit talented and experienced security professionals to help protect their assets and remain competitive. As a Certified Information Systems Security Professional (CISSP), you will be seen as a security professional of proven ability who has successfully met a predefined standard of knowledge and experience that is well understood and respected throughout the industry. By keeping this certification current, you will demonstrate your dedication to staying abreast of security developments.

Consider some of the reasons for attaining a CISSP certification:

- To broaden your current knowledge of security concepts and practices
- To demonstrate your expertise as a seasoned security professional
- To become more marketable in a competitive workforce
- To increase your salary and be eligible for more employment opportunities
- To bring improved security expertise to your current occupation
- To show a dedication to the security discipline

The CISSP certification helps organizations identify which individuals have the ability, knowledge, and experience necessary to implement solid security practices; perform risk analysis; identify necessary countermeasures; and help the organization as a whole protect its facility, network, systems, and information. The CISSP certification also shows potential employers you have achieved a level of proficiency and expertise in skill sets and knowledge required by the security industry. The increasing importance placed on security by organizations of all sizes will only continue in the future, leading to even greater demands for highly skilled security professionals. The CISSP certification shows that a respected third-party organization has recognized an individual's technical and theoretical knowledge and expertise, and distinguishes that individual from those who lack this level of knowledge.

Understanding and implementing security practices is an essential part of being a good network administrator, programmer, or engineer. Job descriptions that do not specifically target security professionals still often require that a potential candidate have a good understanding of security concepts and how to implement them. Due to staff size and budget restraints, many organizations can't afford separate network and security staffs. But they still believe security is vital to their organization. Thus, they often try to combine knowledge of technology and security into a single role. With a CISSP designation, you can put yourself head and shoulders above other individuals in this regard.

The CISSP Exam

Because the CISSP exam covers the eight domains making up the CISSP CBK, it is often described as being “an inch deep and a mile wide,” a reference to the fact that many questions on the exam are not very detailed and do not require you to be an expert in every subject. However, the questions do require you to be familiar with many *different* security subjects.

The CISSP exam comes in two versions depending on the language in which the test is written. The English version uses Computerized Adaptive Testing (CAT) in which the number of questions you are asked depends on your measured level of knowledge but ranges from 100 to 150. Of these, 25 questions will not count toward your score, as they are being evaluated for inclusion in future exams (this is why they are sometimes called pre-test questions). Essentially, the easier it is for the test software to determine your level of proficiency, the fewer questions you’ll get. Regardless of how many questions you are presented, though, you will have no more than three hours to complete the test. When the system has successfully assessed your level of knowledge, the test will end regardless of how long you’ve been at it.



EXAM TIP CAT questions are intentionally designed to “feel” hard (based on the system’s estimate of your knowledge), so don’t be discouraged. Just don’t get bogged down because you must answer at least 100 questions in three hours.

The non-English version of the CISSP exam is also computer-based but is linear, fixed-form (not adaptive) and comprises 250 questions, which must be answered in no more than six hours. Like the CAT version, 25 questions are pre-test (unscored), so you will be graded on the other 225 questions. The 25 research questions are integrated into the exam, so you won’t know which go toward your final grade.

Regardless of which version of the exam you take, you need a score of 700 points out of a possible 1,000. In both versions, you can expect multiple choice and innovative questions. Innovative questions incorporate drag-and-drop (i.e., take a term or item and drag it to the correct position in the frame) or hotspot (i.e., click the item or term that correctly answers the question) interfaces, but are otherwise weighed and scored just like any other question. The questions are pulled from a much larger question bank to ensure the exam is as unique as possible for each examinee. In addition, the test bank constantly changes and evolves to more accurately reflect the real world of security. The exam questions are continually rotated and replaced in the bank as necessary. Questions are weighted based on their difficulty; not all questions are worth the same number of points. The exam is not product or vendor oriented, meaning no questions will be specific to certain products or vendors (for instance, Windows, Unix, or Cisco). Instead, you will be tested on the security models and methodologies used by these types of systems.



EXAM TIP There is no penalty for guessing. If you can’t come up with the right answer in a reasonable amount of time, then you should guess and move on to the next question.

(ISC)², which stands for International Information Systems Security Certification Consortium, also includes scenario-based questions in the CISSP exam. These questions

present a short scenario to the test taker rather than asking the test taker to identify terms and/or concepts. The goal of the scenario-based questions is to ensure that test takers not only know and understand the concepts within the CBK but also can apply this knowledge to real-life situations. This is more practical because in the real world you won't be challenged by having someone asking you, "What is the definition of collusion?" You need to know how to detect and prevent collusion from taking place, in addition to knowing the definition of the term.

After passing the exam, you will be asked to supply documentation, supported by a sponsor, proving that you indeed have the type of experience required to obtain CISSP certification. The sponsor must sign a document vouching for the security experience you are submitting. So, make sure you have this sponsor lined up prior to registering for the exam and providing payment. You don't want to pay for and pass the exam, only to find you can't find a sponsor for the final step needed to achieve your certification.

The reason behind the sponsorship requirement is to ensure that those who achieve the certification have real-world experience to offer organizations. Book knowledge is extremely important for understanding theory, concepts, standards, and regulations, but it can never replace hands-on experience. Proving your practical experience supports the relevance of the certification.

A small sample group of individuals selected at random will be audited after passing the exam. The audit consists mainly of individuals from (ISC)² calling on the candidates' sponsors and contacts to verify the test taker's related experience.

One of the factors that makes the CISSP exam challenging is that most candidates, although they work in the security field, are not necessarily familiar with all eight CBK domains. If a security professional is considered an expert in vulnerability testing or application security, for example, she may not be familiar with physical security, cryptography, or forensics. Thus, studying for this exam will broaden your knowledge of the security field.

The exam questions address the eight CBK security domains, which are described in Table 2.

Domain	Description
Security and Risk Management	<p>This domain covers many of the foundational concepts of information systems security. Some of the topics covered include</p> <ul style="list-style-type: none"> • Professional ethics • Security governance and compliance • Legal and regulatory issues • Personnel security policies • Risk management
Asset Security	<p>This domain examines the protection of assets throughout their life cycle. Some of the topics covered include</p> <ul style="list-style-type: none"> • Identifying and classifying information and assets • Establishing information and asset handling requirements • Provisioning resources securely • Managing the data life cycle • Determining data security controls and compliance requirements

Table 2 Security Domains that Make up the CISSP CBK (*continued*)

Domain	Description
Security Architecture and Engineering	<p>This domain examines the development of information systems that remain secure in the face of a myriad of threats. Some of the topics covered include</p> <ul style="list-style-type: none"> • Secure design principles • Security models • Selection of effective controls • Cryptography • Physical security
Communication and Network Security	<p>This domain examines network architectures, communications technologies, and network protocols with the goal of understanding how to secure them. Some of the topics covered include</p> <ul style="list-style-type: none"> • Secure network architectures • Secure network components • Secure communications channels
Identity and Access Management (IAM)	<p>Identity and access management is one of the most important topics in information security. This domain covers the interactions between users and systems as well as between systems and other systems. Some of the topics covered include</p> <ul style="list-style-type: none"> • Controlling physical and logical access to assets • Identification and authentication • Authorization mechanisms • Identity and access provisioning life cycle • Implementing authentication systems
Security Assessment and Testing	<p>This domain examines ways to verify the security of our information systems. Some of the topics covered include</p> <ul style="list-style-type: none"> • Assessment and testing strategies • Testing security controls • Collecting security process data • Analyzing and reporting results • Conducting and facilitating audits
Security Operations	<p>This domain covers the many activities involved in the daily business of maintaining the security of our networks. Some of the topics covered include</p> <ul style="list-style-type: none"> • Investigations • Logging and monitoring • Change and configuration management • Incident management • Disaster recovery
Software Development Security	<p>This domain examines the application of security principles to the acquisition and development of software systems. Some of the topics covered include</p> <ul style="list-style-type: none"> • The software development life cycle • Security controls in software development • Assessing software security • Assessing the security implications of acquired software • Secure coding guidelines and standards

Table 2 Security Domains that Make Up the CISSP CBK (*continued*)

What Does This Book Cover?

This book covers everything you need to know to become an (ISC)²-certified CISSP. It teaches you the hows and whys behind organizations' development and implementation of policies, procedures, guidelines, and standards. It covers network, application, and system vulnerabilities; what exploits them; and how to counter these threats. This book explains physical security, operational security, and why systems implement the security mechanisms they do. It also reviews the U.S. and international security criteria and evaluations performed on systems for assurance ratings, what these criteria mean, and why they are used. This book also explains the legal and liability issues that surround computer systems and the data they hold, including such subjects as computer crimes, forensics, and what should be done to properly prepare computer evidence associated with these topics for court.

While this book is mainly intended to be used as a study guide for the CISSP exam, it is also a handy reference guide for use after your certification.

Tips for Taking the CISSP Exam

Many people feel as though the exam questions are tricky. Make sure to read each question and its answer choices thoroughly instead of reading a few words and immediately assuming you know what the question is asking. Some of the answer choices may have only subtle differences, so be patient and devote time to reading through the question more than once.

A common complaint heard about the CISSP exam is that some questions seem a bit subjective. For example, whereas it might be easy to answer a technical question that asks for the exact mechanism used in Transport Layer Security (TLS) that protects against man-in-the-middle attacks, it's not quite as easy to answer a question that asks whether an eight-foot perimeter fence provides low, medium, or high security. Many questions ask the test taker to choose the "best" approach, which some people find confusing and subjective. These complaints are mentioned here not to criticize (ISC)² and the exam writers, but to help you better prepare for the exam. This book covers all the necessary material for the exam and contains many questions and self-practice tests. Most of the questions are formatted in such a way as to better prepare you for what you will encounter on the actual exam. So, make sure to read all the material in the book, and pay close attention to the questions and their formats. Even if you know the subject well, you may still get some answers wrong—it is just part of learning how to take tests.

In answering many questions, it is important to keep in mind that some things are inherently more valuable than others. For example, the protection of human lives and welfare will almost always trump all other responses. Similarly, if all other factors are equal and you are given a choice between an expensive and complex solution and a simpler and cheaper one, the second will win most of the time. Expert advice (e.g., from an attorney) is more valuable than that offered by someone with lesser credentials. If one of the possible responses to a question is to seek or obtain advice from an expert, pay close attention to that question. The correct response may very well be to seek out that expert.

Familiarize yourself with industry standards and expand your technical knowledge and methodologies outside the boundaries of what you use today. We cannot stress enough that being the “top dog” in your particular field doesn’t mean you are properly prepared for all eight domains the exam covers.

When you take the CISSP exam at the Pearson VUE test center, other certification exams may be taking place simultaneously in the same room. Don’t feel rushed if you see others leaving the room early; they may be taking a shorter exam.

How to Use This Book

Much effort has gone into putting all the necessary information into this book. Now it’s up to you to study and understand the material and its various concepts. To best benefit from this book, you might want to use the following study method:

- Study each chapter carefully and make sure you understand each concept presented. Many concepts must be fully understood, and glossing over a couple here and there could be detrimental to your success on the exam. The CISSP CBK contains hundreds of individual topics, so take the time needed to understand them all.
- Make sure to study and answer all of the questions. If any questions confuse you, go back and study the corresponding sections again. Remember, you will encounter questions on the actual exam that do not seem straightforward. Do not ignore the confusing questions, thinking they’re not well worded. Instead, pay even closer attention to them because they are included for a reason.
- If you are not familiar with specific topics, such as firewalls, laws, physical security, or protocol functionality, use other sources of information (books, articles, and so on) to attain a more in-depth understanding of those subjects. Don’t just rely solely on what you think you need to know to pass the CISSP exam.
- After reading this book, study the questions and answers, and take the practice tests. Then review the (ISC)² exam objectives and make sure you are comfortable with each bullet item presented. If you are not comfortable with some items, revisit the chapters in which they are covered.
- If you have taken other certification exams—such as Cisco or Microsoft—you might be used to having to memorize details and configuration parameters. But remember, the CISSP test is “an inch deep and a mile wide,” so make sure you understand the concepts of each subject *before* trying to memorize the small, specific details.
- Remember that the exam is looking for the “best” answer. On some questions test takers do not agree with any or many of the answers. You are being asked to choose the best answer out of the four being offered to you.

PART I

Security and Risk Management

- **Chapter 1** Cybersecurity Governance
- **Chapter 2** Risk Management
- **Chapter 3** Compliance
- **Chapter 4** Frameworks

This page intentionally left blank

Cybersecurity Governance

This chapter presents the following:

- Fundamental cybersecurity concepts
- Security governance principles
- Security policies, standards, procedures, and guidelines
- Personnel security policies and procedures
- Security awareness, education, and training

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts.

—Eugene H. Spafford

While some of us may revel in thinking about and implementing cybersecurity, the fact is that most organizations would much rather focus on many other things. Businesses exist to generate profits for their shareholders. Most nonprofit organizations are dedicated to furthering particular social causes such as charity, education, or religion. Apart from security service providers, organizations don't exist specifically to deploy and maintain firewalls, intrusion detection systems, identity management technologies, and encryption devices. No corporation really wants to develop hundreds of security policies, deploy antimalware products, maintain vulnerability management systems, constantly update its incident response capabilities, and have to comply with the myriad of security laws, regulations, and standards that exist worldwide. Business owners would like to be able to make their widgets, sell their widgets, and go home with a nice profit in their pockets. But things are not that simple.

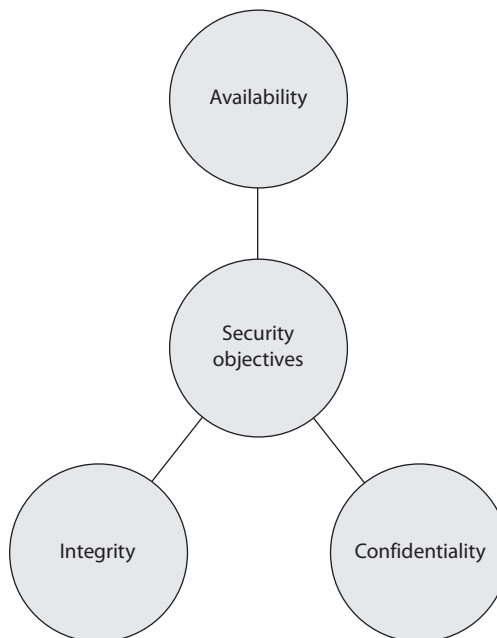
Organizations are increasingly faced with attackers who want to steal customer data to carry out identity theft and banking fraud. Company secrets are commonly being stolen by internal and external entities for economic espionage purposes. Systems are being hijacked and used within botnets to attack other organizations, mine cryptocurrencies, or spread spam. Company funds are being secretly siphoned off through complex and hard-to-identify digital methods, commonly by organized criminal rings in different countries. And organizations that find themselves in the crosshairs of attackers may come under constant attack that brings their systems and websites offline for hours or days. Companies are required to practice a wide range of security disciplines today to keep

their market share, protect their customers and bottom line, stay out of jail, and still sell their widgets.

As we start our exploration of the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) in this chapter, we will define what cybersecurity means and how it must be governed by, well, CISSPs. Each organization must develop an enterprise-wide security program that consists of technologies, procedures, and processes covered throughout this book. As you go along in your security career, you will find that most organizations have some (but rarely all) pieces to the puzzle of an “enterprise-wide security program” in place. Many of the security programs in place today can be thought of as lopsided or lumpy. The security programs excel within the disciplines that the team is most familiar with, and the other disciplines are found lacking. It is your responsibility to become as well rounded in security as possible so that you can identify these deficiencies in security programs and help improve upon them. This is why the CISSP exam covers a wide variety of technologies, methodologies, and processes—you must know and understand them holistically if you are going to help an organization carry out security holistically.

Fundamental Cybersecurity Concepts and Terms

As cybersecurity professionals, our efforts are ultimately focused on the protection of our information systems. These systems consist of people, processes, and technologies designed to operate on information. To protect them means to ensure the confidentiality, integrity, and availability (the CIA triad) of all assets in our information systems as well as the authenticity and nonrepudiation of tasks performed in them. Each asset will require different levels of these types of protection, as we will see in the following sections.



Confidentiality

Confidentiality means keeping unauthorized entities (be they people or processes) from gaining access to information assets. It ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of secrecy should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination. Confidentiality can be provided by encrypting data as it is stored and transmitted, by enforcing strict access control and data classification, and by training personnel on the proper data protection procedures.

Attackers can thwart confidentiality mechanisms by network monitoring, shoulder surfing, stealing credentials, breaking encryption schemes, and social engineering. These topics will be addressed in more depth in later chapters, but briefly, *shoulder surfing* is when a person looks over another person's shoulder and watches their keystrokes or views data as it appears on a computer screen. *Social engineering* is when one person tricks another person into sharing confidential information, for example, by posing as someone authorized to have access to that information. Social engineering can take many forms. Any one-to-one communication medium can be used to perform social engineering attacks.

Users can intentionally or accidentally disclose sensitive information by not encrypting it before sending it to another person, by falling prey to a social engineering attack, by sharing a company's trade secrets, or by not using extra care to protect confidential information when processing it.

Integrity

Integrity means that an asset is free from unauthorized alterations. Only authorized entities should be able to modify an asset, and only in specific authorized ways. For example, if you are reviewing orders placed by customers on your online store, you should not be able to increase the price of any items in those orders after they have been purchased. It is your store, so you can clearly change prices as you wish. You just shouldn't be able to do it after someone agrees to buy an item at a certain price and gives you authorization to charge their credit card.

Environments that enforce and provide this attribute of security ensure that attackers, or mistakes by users, do not compromise the integrity of systems or data. When an attacker inserts malware or a back door into a system, the system's integrity is compromised. This can, in turn, harm the integrity of information held on the system by way of corruption, malicious modification, or the replacement of data with incorrect data. Strict access controls, intrusion detection, and hashing can combat these threats.

Authorized users can also affect a system or its data's integrity by mistake (although internal users may also commit malicious deeds). For example, a user with a full hard drive may unwittingly delete a configuration file under the mistaken assumption that deleting a file must be okay because the user doesn't remember ever using it. Or a user may insert incorrect values into a data-processing application that ends up charging a customer \$3,000 instead of \$300. Incorrectly modifying data kept in databases is another common way users may accidentally corrupt data—a mistake that can have lasting effects.

Security should streamline users' capabilities and give them only certain choices and functionality, so errors become less common and less devastating. System-critical files

should be restricted from viewing and access by users. Applications should provide mechanisms that check for valid and reasonable input values. Databases should let only authorized individuals modify data, and data in transit should be protected by encryption or other mechanisms.

Availability

Availability protection ensures reliable and timely access to data and resources to authorized individuals. Network devices, computers, and applications should provide adequate functionality to perform in a predictable manner with an acceptable level of performance. They should be able to recover from disruptions in a secure and quick fashion, so productivity is not negatively affected. Necessary protection mechanisms must be in place to protect against inside and outside threats that could affect the availability and productivity of all business-processing components.

Like many things in life, ensuring the availability of the necessary resources within an organization sounds easier to accomplish than it really is. Networks have many pieces that must stay up and running (routers, switches, proxies, firewalls, and so on). Software has many components that must be executing in a healthy manner (operating system, applications, antimalware software, and so forth). And an organization's operations can potentially be negatively affected by environmental aspects (such as fire, flood, HVAC issues, or electrical problems), natural disasters, and physical theft or attacks. An organization must fully understand its operational environment and its availability weaknesses so that it can put in place the proper countermeasures.

Authenticity

One of the curious features of the modern Internet is that sometimes we are unsure of who is putting out the things we read and download. Does that patch really come from Microsoft? Did your boss really send you that e-mail asking you to buy \$10,000 worth of gift cards? *Authenticity* protections ensure we can trust that something comes from its claimed source. This concept is at the heart of authentication, which establishes that an entity trying to log into a system is really who it claims to be.

Authenticity in information systems is almost always provided through cryptographic means. As an example, when you connect to your bank's website, the connection should be encrypted using Transport Layer Security (TLS), which in turn uses your bank's digital certificate to authenticate to your browser that it truly is that bank on the other end and not an impostor. When you log in, the bank takes a cryptographic hash of the credentials you provide and compares them to the hash the bank has in your records to ensure it really is you on the other end.

Nonrepudiation

While authenticity establishes that an entity is who it claims to be at a particular point in time, it doesn't really provide historical proof of what that entity did or agreed to. For example, suppose Bob logs into his bank and then applies for a loan. He doesn't read the fine print until later, at which point he decides he doesn't like the terms of the transaction,

so he calls up the bank to say he never signed the contract and to please make it go away. Although the session was authenticated, Bob could claim that he walked away from his computer while logged into the bank's website, that his cat walked over the keyboard and stepped on ENTER, executing the transaction, and that Bob never intended to sign the loan application. It was the cat. Sadly, his claim could hold up in court.

Nonrepudiation, which is closely related to authenticity, means that someone cannot disavow being the source of a given action. For example, suppose Bob's bank had implemented a procedure for loan applications that required him to "sign" the application by entering his personal identification number (PIN). Now the whole cat defense falls apart unless Bob could prove he trained his cat to enter PINs.

Most commonly, nonrepudiation is provided through the use of digital signatures. Just like your physical signature on a piece of paper certifies that you either authored it or agree to whatever is written on it (e.g., a contract), the digital version attests to your sending an e-mail, writing software, or agreeing to a contract. We'll discuss digital signatures later in this book, but for now it will be helpful to remember that they are cryptographic products that, just like an old-fashioned physical signature, can be used for a variety of purposes.



EXAM TIP A good way to differentiate authenticity and nonrepudiation is that authenticity proves to *you* that you're talking to a given person at a given point in time. Nonrepudiation proves to *anyone* that a given person did or said something in the past.

Balanced Security

In reality, when information security is considered, it is commonly only through the lens of keeping secrets secret (confidentiality). The integrity and availability threats tend to be overlooked and only dealt with after they are properly compromised. Some assets have a critical confidentiality requirement (e.g., company trade secrets), some have critical integrity requirements (e.g., financial transaction values), and some have critical availability requirements (e.g., e-commerce web servers). Many people understand the concepts of the CIA triad, but may not fully appreciate the complexity of implementing the necessary controls to provide all the protection these concepts cover. The following provides a *short* list of some of these controls and how they map to the components of the CIA triad.

Availability:

- Redundant array of independent disks (RAID)
- Clustering
- Load balancing
- Redundant data and power lines
- Software and data backups

- Disk shadowing
- Co-location and offsite facilities
- Rollback functions
- Failover configurations

Integrity:

- Hashing (data integrity)
- Configuration management (system integrity)
- Change control (process integrity)
- Access control (physical and technical)
- Software digital signing
- Transmission cyclic redundancy check (CRC) functions

Confidentiality:

- Encryption for data at rest (whole disk, database encryption)
- Encryption for data in transit (IPSec, TLS, PPTP, SSH, described in Chapter 4)
- Access control (physical and technical)

All of these control types will be covered in this book. What is important to realize at this point is that while the concept of the CIA triad may seem simplistic, meeting its requirements is commonly more challenging.

Other Security Terms

The words “vulnerability,” “threat,” “risk,” and “exposure” are often interchanged, even though they have different meanings. It is important to understand each word’s definition and the relationships between the concepts they represent.

A *vulnerability* is a weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

A *threat* is any potential danger that is associated with the exploitation of a vulnerability. If the threat is that someone will identify a specific vulnerability and use it against the organization or individual, then the entity that takes advantage of a vulnerability is referred to as a *threat agent* (or *threat actor*). A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy, or an employee circumventing controls in order to copy files to a medium that could expose confidential information.

A *risk* is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact. If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method. If users are not educated on processes and procedures, there is a higher likelihood that an employee will make an unintentional mistake that may destroy data. If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

An *exposure* is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages. If password management is lax and password rules are not enforced, the organization is exposed to the possibility of having users' passwords compromised and used in an unauthorized manner. If an organization does not have its wiring inspected and does not put proactive fire prevention steps into place, it exposes itself to potentially devastating fires.

A *control*, or *countermeasure*, is put into place to mitigate (reduce) the potential risk. A countermeasure may be a software configuration, a hardware device, or a procedure that eliminates a vulnerability or that reduces the likelihood a threat agent will be able to exploit a vulnerability. Examples of countermeasures include strong password management, firewalls, a security guard, access control mechanisms, encryption, and security awareness training.



NOTE The terms “control,” “countermeasure,” and “safeguard” are interchangeable terms. They are mechanisms put into place to reduce risk.

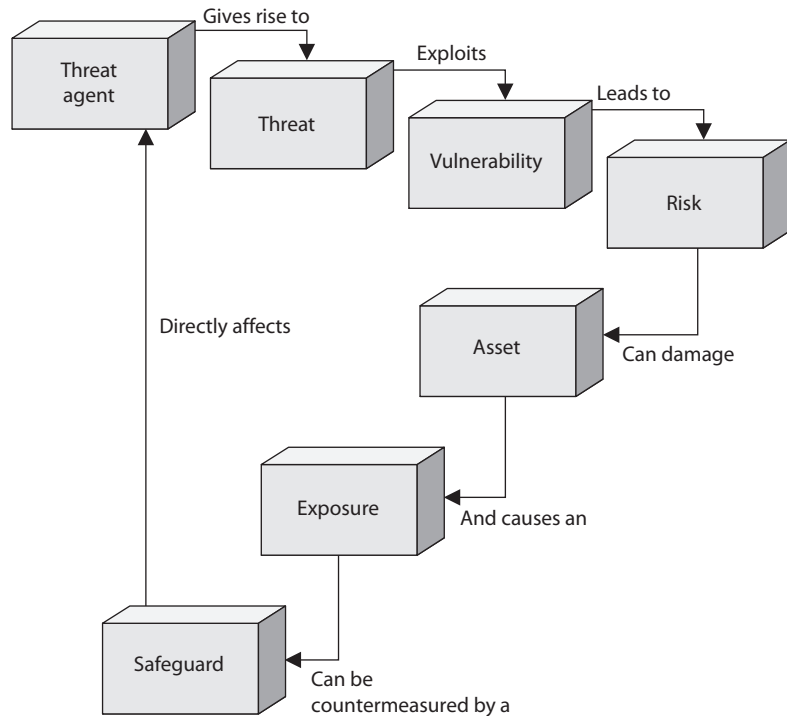
If an organization has antimalware software but does not keep the signatures up to date, this is a vulnerability. The organization is vulnerable to more recent malware attacks. The threat is that a threat agent will insert malware into the environment and disrupt productivity. The risk is the likelihood of a threat agent using malware in the environment and the resulting potential damage. If this happens, then a vulnerability has been exploited and the organization is exposed to loss. The countermeasures in this situation are to update the signatures and install the antimalware software on all computers. The relationships among risks, vulnerabilities, threats, and countermeasures are shown in Figure 1-1.

Applying the right countermeasure can eliminate the vulnerability and exposure, and thus reduce the risk. The organization cannot eliminate the threat agent, but it can protect itself and prevent this threat agent from exploiting vulnerabilities within the environment.

Many people gloss over these basic terms with the idea that they are not as important as the sexier things in information security. But you will find that unless a security team has an agreed-upon language in place, confusion will quickly take over. These terms embrace the core concepts of security, and if they are confused in any manner, then the activities that are rolled out to enforce security are commonly confused.

Figure 1-1

The relationships among the different security concepts



Security Governance Principles

Now that we have established a shared vocabulary for the fundamental cybersecurity concepts and understand how they relate to each other, let's turn our attention to how we can prioritize, assess, and continuously improve the security of our organizations. This is where security governance comes into play. *Security governance* is a framework that supports the security goals of an organization being set and expressed by senior management, communicated throughout the different levels of the organization, and consistently applied and assessed. Security governance grants power to the entities who need to implement and enforce security and provides a way to verify the performance of these necessary security activities. Senior management not only needs to set the direction of security but also needs a way to be able to view and understand how their directives are being met or not being met.

If a board of directors and CEO demand that security be integrated properly at all levels of the organization, how do they know it is really happening? Oversight mechanisms must be developed and integrated so that the people who are ultimately responsible for an organization are constantly and consistently updated on the overall health and security posture of the organization. This happens through properly defined communication channels, standardized reporting methods, and performance-based metrics.

Let's compare two companies. Company A has an effective security governance program in place and Company B does not. Now, to the untrained eye it would seem

as though Companies A and B are equal in their security practices because they both have security policies, procedures, and standards in place, the same security technology controls (firewalls, endpoint detection, identity management, and so on), defined security roles, and security awareness training. You may think, “These two companies are on the ball and quite evolved in their security programs.” But if you look closer, you will see some critical differences (listed in Table 1-1).

Does the organization you work for look like Company A or Company B? Most organizations today have many of the pieces and parts to a security program (policies, standards, firewalls, security team, IDS, and so on), but management may not be

Company A	Company B
Board members understand that information security is critical to the company and demand to be updated quarterly on security performance and breaches.	Board members do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.
The chief executive officer (CEO), chief financial officer (CFO), chief information officer (CIO), chief information security officer (CISO), and business unit managers participate in a risk management committee that meets each month, and information security is always one topic on the agenda to review.	The CEO, CFO, and business unit managers feel as though information security is the responsibility of the CIO, CISO, and IT department and do not get involved.
Executive management sets an acceptable risk level that is the basis for the company's security policies and all security activities.	The CISO copied some boilerplate security policies, inserted his company's name, and had the CEO sign them.
Executive management holds business unit managers responsible for carrying out risk management activities for their specific business units.	All security activity takes place within the security department; thus, security works within a silo and is not integrated throughout the organization.
Critical business processes are documented along with the risks that are inherent at the different steps within the business processes.	Business processes are not documented and not analyzed for potential risks that can affect operations, productivity, and profitability.
Employees are held accountable for any security breaches they participate in, either maliciously or accidentally.	Policies and standards are developed, but no enforcement or accountability practices have been envisioned or deployed.
Security products, managed services, and consulting services are purchased and deployed in an informed manner. They are also constantly reviewed to ensure they are cost-effective.	Security products, managed services, and consulting services are purchased and deployed without any real research or performance metrics to determine the return on investment or effectiveness.
The organization is continuing to review its processes, including security, with the goal of continued improvement.	The organization does not analyze its performance for improvement, but continually marches forward and makes similar mistakes over and over again.

Table 1-1 Security Governance Program: A Comparison of Two Companies

truly involved, and security has not permeated throughout the organization. Some organizations rely just on technology and isolate all security responsibilities within the IT group. If security were just a technology issue, then this security team could properly install, configure, and maintain the products, and the company would get a gold star and pass the audit with flying colors. But that is not how information security works. It is much more than just technological solutions. Security must be driven throughout the organization, and having several points of responsibility and accountability is critical.

At this point, you may be asking, “So, what does security governance actually look like in the real world?” Security governance is typically implemented as a formal cybersecurity program or an information security management system (ISMS). Whichever of these names you call it, it is a collection of policies, procedures, baselines, and standards that an organization puts in place to make sure that its security efforts are aligned with business needs, streamlined, and effective, and that no security controls are missing. Figure 1-2 illustrates many of the elements that go into a complete security program.

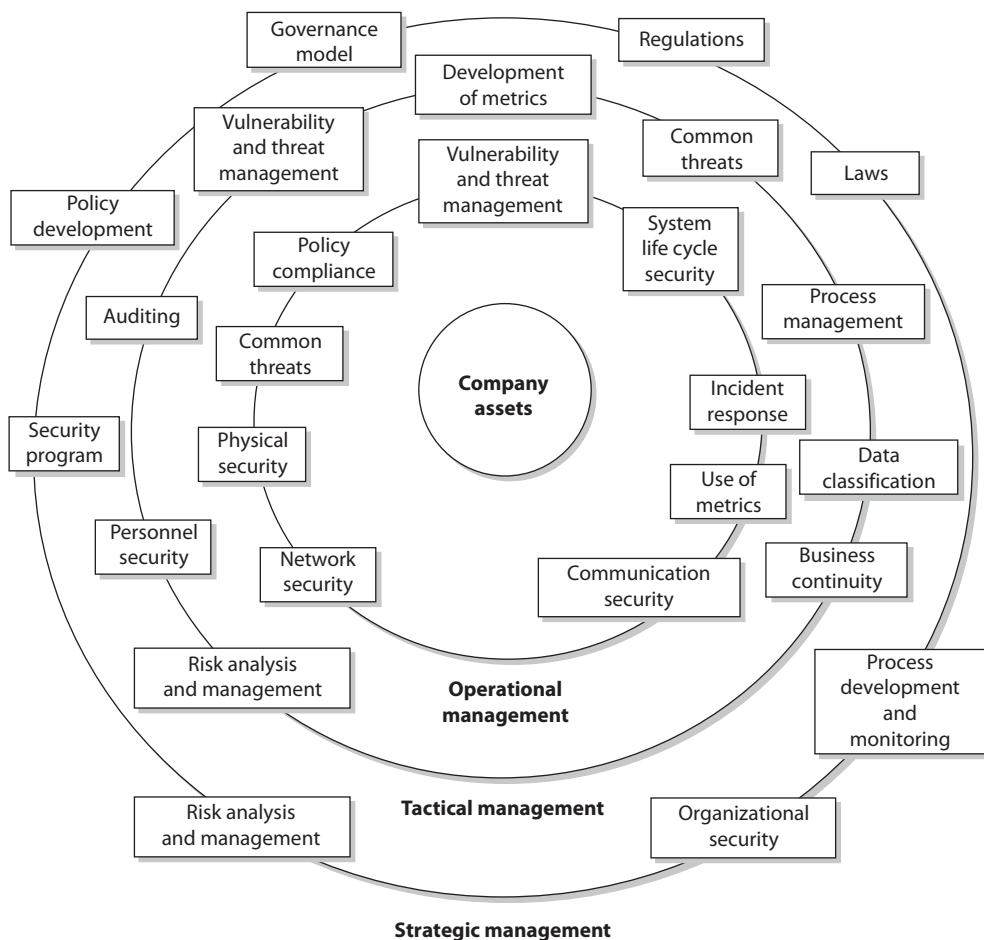


Figure 1-2 A complete security program contains many items.

Aligning Security to Business Strategy

An *enterprise security architecture* is a subset of an enterprise architecture (discussed in depth in Chapter 4) and implements an information security strategy. It consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally. It is a comprehensive and rigorous method for describing the structure and behavior of all the components that make up a holistic ISMS. The main reason to develop an enterprise security architecture is to ensure that security efforts align with business practices in a standardized and cost-effective manner. The architecture works at an abstraction level and provides a frame of reference. Besides security, this type of architecture allows organizations to better achieve interoperability, integration, ease of use, standardization, and governance.

How do you know if an organization does not have an enterprise security architecture in place? If the answer is “yes” to most of the following questions, this type of architecture is not in place:

- Does security take place in silos throughout the organization?
- Is there a continual disconnect between senior management and the security staff?
- Are redundant products purchased for different departments for overlapping security needs?
- Is the security program made up of mainly policies without actual implementation and enforcement?
- When a user’s access requirements increase because of business needs, does the network administrator just modify the access controls without the user manager’s documented approval?
- When a new product is being rolled out, do unexpected interoperability issues pop up that require more time and money to fix?
- Do many “one-off” efforts take place instead of following standardized procedures when security issues arise?
- Are the business unit managers unaware of their security responsibilities and how their responsibilities map to legal and regulatory requirements?
- Is “sensitive data” defined in a policy, but the necessary controls are not fully implemented and monitored?
- Are stovepipe (point) solutions implemented instead of enterprise-wide solutions?
- Are the same expensive mistakes continuing to take place?
- Is security governance currently unavailable because the enterprise is not viewed or monitored in a standardized and holistic manner?
- Are business decisions being made without taking security into account?
- Are security personnel usually putting out fires with no real time to look at and develop strategic approaches?
- Are some business units engaged in security efforts that other business units know nothing about?

If many of these answers are “yes,” no useful architecture is in place. Now, the following is something very interesting the authors have seen over several years. Most organizations have multiple problems in the preceding list and yet they focus on each item as if it is unconnected to the other problems. What the CSO, CISO, and/or security administrator does not always understand is that these are just *symptoms* of a treatable disease. The “treatment” is to put one person in charge of a team that develops a phased-approach enterprise security architecture rollout plan. The goals are to integrate technology-oriented and business-centric security processes; link administrative, technical, and physical controls to properly manage risk; and integrate these processes into the IT infrastructure, business processes, and the organization’s culture.

A helpful tool for aligning an organization’s security architecture with its business strategy is the *Sherwood Applied Business Security Architecture (SABSA)*, which is shown in Table 1-2. It is a layered framework, with its first layer describing the business context within which the security architecture must exist. Each layer of the framework decreases in abstraction and increases in detail, so it builds upon the others and moves from policy to practical implementation of technology and solutions. The idea is to provide a chain of traceability through the contextual, conceptual, logical, physical, component, and operational levels.

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetimes and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices, and procedures	Security mechanisms	Users, applications, and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions, and ACLs	Processes, nodes, addresses, and protocols	Security step timing and sequencing
Operational	Assurance of operation continuity	Operation risk management	Security service management and support	Application and user management and support	Security of sites, networks, and platforms	Security operations schedule

Table 1-2 SABSA Architecture Framework

The following outlines the questions that are to be asked and answered at each level of the framework:

- **What are you trying to do at this layer?** The assets to be protected by your security architecture.
- **Why are you doing it?** The motivation for wanting to apply security, expressed in the terms of this layer.
- **How are you trying to do it?** The functions needed to achieve security at this layer.
- **Who is involved?** The people and organizational aspects of security at this layer.
- **Where are you doing it?** The locations where you apply your security, relevant to this layer.
- **When are you doing it?** The time-related aspects of security relevant to this layer.

SABSA is a framework and methodology for enterprise security architecture and service management. Since it is a *framework*, this means it provides a structure for individual architectures to be built from. Since it is a *methodology* also, this means it provides the processes to follow to build and maintain this architecture. SABSA provides a life-cycle model so that the architecture can be constantly monitored and improved upon over time.



EXAM TIP You do not need to memorize the SABSA framework, but you do need to understand how security programs align with business strategies.

For an enterprise security architecture to be successful in its development and implementation, the following items must be understood and followed: strategic alignment, business enablement, process enhancement, and security effectiveness. We'll cover the first three of these in the following sections but will cover security effectiveness in Chapter 18 when we discuss security assessments.

Strategic Alignment

Strategic alignment means the business drivers and the regulatory and legal requirements are being met by the enterprise security architecture. Security efforts must provide and support an environment that allows an organization to not only survive, but thrive. The security industry has grown up from the technical and engineering world, not the business world. In many organizations, while the IT security personnel and business personnel might be located physically close to each other, they are commonly worlds apart in how they see the same organization they work in. Technology is only a tool that supports a business; it is not the business itself. The IT environment is analogous to the circulatory system within a human body; it is there to support the body—the body does not exist to support the circulatory system. And security is analogous to the immune system of the body—it is there to protect the overall environment. If these critical systems (business, IT, security)

do not work together in a concerted effort, there will be deficiencies and imbalances. While deficiencies and imbalances lead to disease in the body, deficiencies and imbalances within an organization can lead to risk and security compromises.

Business Enablement

When looking at the *business enablement* requirement of the enterprise security architecture, we need to remind ourselves that each organization exists for one or more specific business purposes. Publicly traded companies are in the business of increasing shareholder value. Nonprofit organizations are in the business of furthering a specific set of causes. Government organizations are in the business of providing services to their citizens. Companies and organizations do not exist for the sole purpose of being secure. Security cannot stand in the way of business processes, but should be implemented to better enable them.

Business enablement means the core business processes are integrated into the security operating model—they are standards based and follow a risk tolerance criteria. What does this mean in the real world? Let's say a company's accountants have figured out that if they allow the customer service and support staff to work from home, the company would save a lot of money on office rent, utilities, and overhead—plus, the company's insurance would be cheaper. The company could move into this new model with the use of virtual private networks (VPNs), firewalls, content filtering, and so on. Security enables the company to move to this different working model by providing the necessary protection mechanisms. If a financial institution wants to enable its customers to view bank account information and carry out money transfers online, it can offer this service if the correct security mechanisms are put in place (access control, authentication, secure connections, etc.). Security should help the organization thrive by providing the mechanisms to do new things safely.

Process Enhancement

Process enhancement can be quite beneficial to an organization if it takes advantage of this capability when it is presented to it. An organization that is serious about securing its environment will have to take a close look at many of the business processes that take place on an ongoing basis. Many times, these processes are viewed through the eye-glasses of security, because that's the reason for the activity, but this is a perfect chance to enhance and improve upon the same processes to increase productivity. When you look at many business processes taking place in all types of organizations, you commonly find a duplication of efforts, manual steps that can be easily automated, or ways to streamline and reduce time and effort that are involved in certain tasks. This is commonly referred to as *process reengineering*.

When an organization is developing its security enterprise components, those components must be integrated into the business processes to be effective. This can allow for process management to be refined and calibrated. This, in turn, allows for security to be integrated in system life cycles and day-to-day operations. So, while business enablement means "we can do new stuff," process enhancement means "we can do stuff better."

Organizational Processes

The processes we just covered are regular day-to-day ones. There are other processes that happen less frequently but may have a much more significant impact on the security posture of the organization. Let's dig a bit deeper into some of these key organizational processes and how our security efforts align with, enable, and enhance them.

Mergers and Acquisitions

As companies grow, they often acquire new capabilities (e.g., markets, products, and intellectual property) by merging with another company or outright acquiring it. *Mergers and acquisitions (M&A)* always take place for business reasons, but they almost always have significant cybersecurity implications. Think of it this way: your company didn't acquire only the business assets of that other company it just purchased; it also acquired its security program and all the baggage that may come with it. Suppose that during the M&A process you discover that the company that your company is acquiring has a significant but previously unknown data breach. This is exactly what happened in 2017 when Verizon acquired Yahoo! and discovered that the latter had experienced two massive security breaches. The acquisition went forward, but at a price that was \$350 million lower than originally agreed.

One of the ways in which companies protect themselves during a merger or acquisition is by conducting extensive audits of the company they are about to merge with or acquire. There are many service providers who now offer *compromise assessments*, which are in-depth technical examinations of a company's information systems to determine whether an undocumented compromise is ongoing or has happened in the past. It's sort of like exploratory surgery; let's open up the patient and see what we find. Another approach is to conduct an audit of the ISMS, which is more focused on policies, procedures, and controls.

Divestitures

A *divestiture*, on the other hand, is when your company sells off (or otherwise gets rid of) a part of itself. There are many reasons why a company may want to divest itself of a business asset, such as having a business unit that is not profitable or no longer well aligned with the overarching strategy. If the divestiture involves a sale or transfer of an asset to another company, that company is going to audit that asset. In other words, for us cybersecurity professionals, a divestiture is when we have to answer tough questions from the buyer, and an M&A is when we are the ones asking the tough questions of someone else. They are two sides to the same coin.

If your company is divesting assets for whose security you are responsible, you will probably work closely with the business and legal teams to identify any problem areas that might reduce the value of the assets being sold. For example, if there are any significant vulnerabilities in those assets, you may want to apply controls to mitigate the related risks. If you discover a compromise, you want to eradicate it and recover from it aggressively.

A less obvious cybersecurity implication of divestiture is the need to segment the part or parts of the ISMS that involve the asset(s) in question. If your company is selling a

business unit, it undoubtedly has security policies, procedures, and controls that apply to it but may also apply to other business areas. Whoever is acquiring the assets will want to know what those are, and maybe even test them at a technical level. You need to be prepared to be audited without revealing any proprietary or confidential information in the process. Be sure to keep your legal team close to ensure you are responsive to what is required of you, but nothing else.

Governance Committees

The organizational processes we've described so far (M&A and divestitures) are triggered by a business decision to either acquire or get rid of some set of assets. There is another key process that is ongoing in many organizations with mature cybersecurity practices. A *governance committee* is a standing body whose purpose is to review the structures and practices of the organization and report its findings to the board of directors. While it may sound a bit scary to have such a committee watching over everything you do, they can actually be your allies by shining a light on the tough issues that you cannot solve by yourself without help from the board. It is important for you to know who is who in your organization and who can help get what you need to ensure a secure environment.

Organizational Roles and Responsibilities

Senior management and other levels of management understand the vision of the organization, the business goals, and the objectives. The next layer down is the functional management, whose members understand how their individual departments work, what roles individuals play within the organization, and how security affects their department directly. The next layers are operational managers and staff. These layers are closer to the actual operations of the organization. They know detailed information about the technical and procedural requirements, the systems, and how the systems are used. The employees at these layers understand how security mechanisms integrate into systems, how to configure them, and how they affect daily productivity. Every layer offers different insight into what type of role security plays within an organization, and each should have input into the best security practices, procedures, and chosen controls to ensure the agreed-upon security level provides the necessary amount of protection without negatively affecting the company's productivity.



EXAM TIP Senior management always carries the ultimate responsibility for the organization.

Although each layer is important to the overall security of an organization, some specific roles must be clearly defined. Individuals who work in smaller environments (where everyone must wear several hats) may get overwhelmed with the number of roles presented next. Many commercial businesses do not have this level of structure in their security teams, but many large companies, government agencies, and military units do. What you need to understand are the responsibilities that must be assigned and whether

they are assigned to just a few people or to a large security team. These roles include the executive management, security officer, data owner, data custodian, system owner, security administrator, supervisor (user manager), change control analyst, data analyst, user, auditor, and the guy who gets everyone coffee.

Executive Management

The individuals designated as executive management typically are those whose titles start with “chief,” and collectively they are often referred to as the “C-suite.” Executive leaders are ultimately responsible for everything that happens in their organizations, and as such are considered the ultimate business and function owners. This has been evidenced time and again (as we will see shortly) in high-profile cases wherein executives have been fired, sued, or even prosecuted for organizational failures or fraud that occurred under their leadership. Let’s start at the top of a corporate entity, the CEO.

Chief Executive Officer The *chief executive officer (CEO)* has the day-to-day management responsibilities of an organization. This person is often the chairperson of the board of directors and is the highest-ranking officer in the company. This role is for the person who oversees the company’s finances, strategic planning, and operations from a high level. The CEO is usually seen as the visionary for the company and is responsible for developing and modifying the company’s business plan. The CEO sets budgets; forms partnerships; and decides on what markets to enter, what product lines to develop, how the company will differentiate itself, and so on. This role’s overall responsibility is to ensure that the company grows and thrives.



NOTE The CEO can delegate tasks, but not necessarily responsibility. More and more regulations dealing with information security are holding the CEO accountable for ensuring the organization practices due care and due diligence with respect to information security, which is why security departments across the land are receiving more funding. Personal liability for the decision makers and purse-string holders has loosened those purse strings, and companies are now able to spend more money on security than before. (Due care and due diligence are described in detail in Chapter 3.)

Chief Financial Officer The *chief financial officer (CFO)* is responsible for the corporation’s accounting and financial activities and the overall financial structure of the organization. This person is responsible for determining what the company’s financial needs will be and how to finance those needs. The CFO must create and maintain the company’s capital structure, which is the proper mix of equity, credit, cash, and debt financing. This person oversees forecasting and budgeting and the processes of submitting financial statements to the regulators and stakeholders.

Chief Information Officer The *chief information officer (CIO)* may report to either the CEO or CFO, depending upon the corporate structure, and is responsible for the strategic use and management of information systems and technology within the organization. Over time, this position has become more strategic and less operational in

Executives and Incarcerations and Fines, Oh My!

The CFO and CEO are responsible for informing stakeholders (creditors, analysts, employees, management, investors) of the firm's financial condition and health. After the corporate debacles at Enron and WorldCom uncovered in 2001–2002, the U.S. government enacted the Sarbanes-Oxley Act (SOX), which prescribes to the CEO and CFO financial reporting responsibilities and includes penalties and potential *personal* liability for failure to comply. SOX gave the Securities Exchange Commission (SEC) more authority to create regulations that ensure these officers cannot simply pass along fines to the corporation for personal financial misconduct. Under SOX, they can personally be fined millions of dollars and/or go to jail. The following list provides a sampling of some of the cases in the past decade in which C-suite executives have been held accountable for cybersecurity issues under various laws:

- **August 2020** Joseph Sullivan, former chief information security officer at Uber, was charged with obstruction of justice and misprision of a felony in connection with the attempted cover-up of the 2016 hack of Uber.
- **July 2019** Facebook agreed to pay \$100M in fines for making misleading disclosures concerning the risks to user data after becoming aware that Cambridge Analytica had improperly collected and misused PII on nearly 30M Facebook users in 2014 and 2015. The company neither admitted nor denied the SEC allegations as part of this agreement.
- **March 2019** Jun Ying, a former chief information officer for Equifax, pled guilty and was subsequently convicted to four months in prison on charges of insider trading for allegedly selling his stock in the company after discovering a massive data breach. He suspected (correctly) that the stock would lose value once the breach became known.
- **March 2018** Martin Shkreli, a notorious pharmaceutical executive, was sentenced to seven years in prison after being convicted of securities fraud stemming from his alleged use of funds from new companies to pay down debts previously incurred by financially troubled companies.
- **December 2017** KIT Digital's former CEO Kaleil Isaza Tuzman was found guilty of market manipulation and fraud charges. His former CFO, Robin Smyth, had previously pled guilty and turned government witness against Tuzman. As of this writing, Tuzman is still awaiting sentencing.
- **June 2015** Joe White, the former CFO of Shelby Regional Medical Center, was sentenced to 23 months in federal prison after making false claims to receive payments under the Medicare Electronic Health Record Incentive Program.

These are only some of the big cases that made it into the headlines. Other executives have also received punishments for “creative accounting” and fraudulent activities.

many organizations. CIOs oversee and are responsible for the day-in, day-out technology operations of a company, but because organizations are so dependent upon technology, CIOs are being asked to sit at the corporate table more and more.

CIO responsibilities have extended to working with the CEO (and other management) on business-process management, revenue generation, and how business strategy can be accomplished with the company's underlying technology. This person usually should have one foot in techno-land and one foot in business-land to be effective because she is bridging two very different worlds.

The CIO sets the stage for the protection of company assets and is ultimately responsible for the success of the company's security program. Direction should be coming down from the CEO, and there should be clear lines of communication between the board of directors, the C-level staff, and mid-management.

Chief Privacy Officer The *chief privacy officer (CPO)* is a newer position, created mainly because of the increasing demands on organizations to protect a long laundry list of different types of data. This role is responsible for ensuring that customer, company, and employee data is kept safe, which keeps the company out of criminal and civil courts and hopefully out of the headlines. This person is often an attorney with privacy law experience and is directly involved with setting policies on how data is collected, protected, and given out to third parties. The CPO often reports to the chief security officer.

It is important that the CPO understand the privacy, legal, and regulatory requirements the organization must comply with. With this knowledge, the CPO can then develop the organization's policies, standards, procedures, controls, and contract agreements to ensure that privacy requirements are being properly met. Remember also that organizations are responsible for knowing how their suppliers, partners, and other third parties are protecting this sensitive information. The CPO may be responsible for reviewing the data security and privacy practices of these other parties.

Some companies have carried out risk assessments without considering the penalties and ramifications they would be forced to deal with if they do not properly protect the information they are responsible for. Without considering these liabilities, risk cannot be properly assessed.

Privacy

Privacy is different from security. *Privacy* indicates the amount of control an individual should be able to have and expect to have as it relates to the release of their own sensitive information. *Security* refers to the mechanisms that can be put into place to provide this level of control.

It is becoming more critical (and more difficult) to protect personally identifiable information (PII) because of the increase of identity theft and financial fraud threats. PII is a combination of identification elements (name, address, phone number, account number, etc.). Organizations must have privacy policies and controls in place to protect their employee and customer PII. Chapter 3 discusses PII in depth.

CSO vs. CISO

The CSO and CISO may have similar or very different responsibilities, depending on the individual organization. In fact, an organization may choose to have both, either, or neither of these roles. It is up to an organization that has either or both of these roles to define their responsibilities. By and large, the CSO role usually has a further-reaching list of responsibilities compared to the CISO role. The CISO is usually focused more on technology and has an IT background. The CSO usually is required to understand a wider range of business risks, including physical security, not just technological risks.

The CSO is usually more of a businessperson and typically is present in larger organizations. If a company has both roles, the CISO reports directly to the CSO.

The CSO is commonly responsible for ensuring *convergence*, which is the formal cooperation between previously disjointed security functions. This mainly pertains to physical and IT security working in a more concerted manner instead of working in silos within the organization. Issues such as loss prevention, fraud prevention, business continuity planning, legal/regulatory compliance, and insurance all have physical security and IT security aspects and requirements. So one individual (CSO) overseeing and intertwining these different security disciplines allows for a more holistic and comprehensive security program.

The organization should document how privacy data is collected, used, disclosed, archived, and destroyed. Employees should be held accountable for not following the organization's standards on how to handle this type of information.

Chief Security Officer The *chief security officer (CSO)* is responsible for understanding the risks that the company faces and for mitigating these risks to an acceptable level. This role is responsible for understanding the organization's business drivers and for creating and maintaining a security program that facilitates these drivers, along with providing security, compliance with a long list of regulations and laws, and any customer expectations or contractual obligations.

The creation of this role is a mark in the "win" column for the security industry because it means security is finally being seen as a business issue. Previously, security was relegated to the IT department and was viewed solely as a technology issue. As organizations began to recognize the need to integrate security requirements and business needs, creating a position for security in the executive management team became more of a necessity. The CSO's job is to ensure that business is not disrupted in any way due to security issues. This extends beyond IT and reaches into business processes, legal issues, operational issues, revenue generation, and reputation protection.

Data Owner

The *data owner* (information owner) is usually a member of management who is in charge of a specific business unit and who is ultimately responsible for the protection

and use of a specific subset of information. The data owner has due-care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data she is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And the data owner will deal with security violations pertaining to the data she is responsible for protecting. The data owner, who obviously has enough on her plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.



NOTE Data ownership takes on a different meaning when outsourcing data storage requirements. You may want to ensure that the service contract includes a clause to the effect that all data is and shall remain the sole and exclusive property of your organization.

Data Custodian

The *data custodian* (information custodian) is responsible for maintaining and protecting the data. This role is usually filled by the IT or security department, and the duties include implementing and maintaining security controls; performing regular backups of the data; periodically validating the integrity of the data; restoring data from backup media; retaining records of activity; and fulfilling the requirements specified in the company's security policy, standards, and guidelines that pertain to information security and data protection.

System Owner

The *system owner* is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure that the systems are

Data Owner Issues

Each business unit should have a data owner who protects the unit's most critical information. The company's policies must give the data owners the necessary authority to carry out their tasks.

This is not a technical role, but rather a business role that must understand the relationship between the unit's success and the protection of this critical asset. Not all businesspeople understand this role, so they should be given the necessary training.

properly assessed for vulnerabilities and must report any that are discovered to the incident response team and data owner.

Security Administrator

The *security administrator* is responsible for implementing and maintaining specific security network devices and software in the enterprise. These controls commonly include firewalls, an intrusion detection system (IDS), intrusion prevention system (IPS), anti-malware, security proxies, data loss prevention, etc. It is common for a delineation to exist between the security administrator's responsibilities and the network administrator's responsibilities. The security administrator has the main focus of keeping the network secure, and the network administrator has the focus of keeping things up and running.

A security administrator's tasks commonly also include creating new system user accounts, implementing new security software, testing security patches and components, and issuing new passwords. The security administrator must make sure access rights given to users support the policies and data owner directives.

Supervisor

The *supervisor* role, also called *user manager*, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security; making sure the employees' account information is up to date; and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

Change Control Analyst

Since the only thing that is constant is change, someone must make sure changes happen securely. The *change control analyst* is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity.

Data Analyst

Having proper data structures, definitions, and organization is very important to a company. The *data analyst* is responsible for ensuring that data is stored in a way that makes the most sense to the company and the individuals who need to access and work with it. For example, payroll information should not be mixed with inventory information; the purchasing department needs to have a lot of its values in monetary terms; and the inventory system must follow a standardized naming scheme. The data analyst may be responsible for architecting a new system that will hold company information or advising in the purchase of a product that will do so. The data analyst works with the data owners to help ensure that the structures set up coincide with and support the company's business objectives.

User

The *user* is any individual who routinely uses the data for work-related tasks. The user must have the necessary level of access to the data to perform the duties within their position and is responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others.

Auditor

The function of the *auditor* is to periodically check that everyone is doing what they are supposed to be doing and to ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations. Organizations can have internal auditors and/or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met.

While many security professionals fear and dread auditors, they can be valuable tools in ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problems.

Why So Many Roles?

Most organizations will not have all the roles previously listed, but what is important is to build an organizational structure that contains the necessary roles and map the correct security responsibilities to them. This structure includes clear definitions of responsibilities, lines of authority and communication, and enforcement capabilities. A clear-cut structure takes the mystery out of who does what and how things are handled in different situations.

Security Policies, Standards, Procedures, and Guidelines

Computers and the information processed on them usually have a direct relationship with a company's critical missions and objectives. Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible. A comprehensive management approach must be developed to accomplish these goals successfully. This is because everyone within an organization may have a different set of personal values and experiences they bring to the environment with regard to security. It is important to make sure everyone is consistent regarding security at a level that meets the needs of the organization.

For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization. Senior management needs to define the scope of security and identify and decide what must be protected and to what extent. Management must understand the business needs and compliance requirements (regulations, laws, and liability issues) for which it is responsible regarding security and ensure that the company as a whole fulfills its obligations. Senior management also must determine what is expected from employees and what the consequences of

noncompliance will be. These decisions should be made by the individuals who will be held ultimately responsible if something goes wrong. But it is a common practice to bring in the expertise of the security officers to collaborate in ensuring that sufficient policies and controls are being implemented to achieve the goals being set and determined by senior management.

A security program contains all the pieces necessary to provide overall protection to an organization and lays out a long-term security strategy. A security program's documentation should be made up of security policies, procedures, standards, guidelines, and baselines. The human resources and legal departments must be involved in the development and enforcement of rules and requirements laid out in these documents.

ISMS vs. Enterprise Security Architecture

What is the difference between an ISMS and an enterprise security architecture? An ISMS outlines the controls that need to be put into place (risk management, vulnerability management, business continuity planning, data protection, auditing, configuration management, physical security, etc.) and provides direction on how those controls should be managed throughout their life cycle. The ISMS specifies the pieces and parts that need to be put into place to provide a holistic security program for the organization overall and how to properly take care of those pieces and parts. The enterprise security architecture illustrates how these components are to be integrated into the different layers of the current business environment. The security components of the ISMS have to be interwoven throughout the business environment and not siloed within individual company departments.

For example, the ISMS will dictate that risk management needs to be put in place, and the enterprise security architecture will chop up the risk management components and illustrate how risk management needs to take place at the strategic, tactical, and operational levels. As another example, the ISMS could dictate that data protection needs to be put into place. The security architecture can show how this happens at the infrastructure, application, component, and business level. At the infrastructure level we can implement data loss protection technology to detect how sensitive data is traversing the network. Applications that maintain sensitive data must have the necessary access controls and cryptographic functionality. The components within the applications can implement the specific cryptographic functions. And protecting sensitive company information can be tied to business drivers, which is illustrated at the business level of the architecture.

The ISO/IEC 27000 series (which outlines the ISMS and is covered in detail in Chapter 4) is very policy oriented and outlines the necessary components of a security program. This means that the ISO standards are general in nature, which is not a defect—they were created that way so that they could be applied to various types of businesses, companies, and organizations. But since these standards are general, it can be difficult to know how to implement them and map them to your company's infrastructure and business needs. This is where the enterprise security architecture comes into play. The architecture is a tool used to ensure that what is outlined in the security standards is implemented throughout the different layers of an organization.

The language, level of detail, formality of the documents, and supporting mechanisms should be examined by the policy developers. Security policies, standards, guidelines, procedures, and baselines must be developed with a realistic view to be most effective. Highly structured organizations usually follow documentation in a more uniform way. Less structured organizations may need more explanation and emphasis to promote compliance. The more detailed the rules are, the easier it is to know when one has been violated. However, overly detailed documentation and rules can prove to be more burdensome than helpful. The business type, its culture, and its goals must be evaluated to make sure the proper language is used when writing security documentation.

There are a lot of legal liability issues surrounding security documentation. If your organization has a policy outlining how it is supposed to be protecting sensitive information and it is found out that your organization is not practicing what it is preaching, criminal charges and civil suits could be filed and successfully executed. It is important that an organization's security does not just look good on paper, but in action also.

Security Policy

A *security policy* is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization. A security policy can be an organizational policy, an issue-specific policy, or a system-specific policy. In an *organizational security policy*, management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out. This policy must address applicable laws, regulations, and liability issues and how they are to be satisfied. The organizational security policy provides scope and direction for all future security activities within the organization. It also describes the amount of risk senior management is willing to accept.

The organizational security policy has several important characteristics that must be understood and implemented:

- Business objectives should drive the policy's creation, implementation, and enforcement. The policy should not dictate business objectives.
- It should be an easily understood document that is used as a reference point for all employees and management.
- It should be developed and used to integrate security into all business functions and processes.
- It should be derived from and support all legislation and regulations applicable to the company.
- It should be reviewed and modified as a company changes, such as through adoption of a new business model, a merger with another company, or change of ownership.
- Each iteration of the policy should be dated and under version control.
- The units and individuals who are governed by the policy must have easy access to it. Policies are commonly posted on portals on an intranet.

- It should be created with the intention of having the policies in place for several years at a time. This will help ensure policies are forward-thinking enough to deal with potential changes that may arise.
- The level of professionalism in the presentation of the policies reinforces their importance, as well as the need to adhere to them.
- It should not contain language that isn't readily understood by everyone. Use clear and declarative statements that are easy to understand and adopt.
- It should be reviewed on a regular basis and adapted to correct incidents that have occurred since the last review and revision of the policies.

A process for dealing with those who choose not to comply with the security policies must be developed and enforced so there is a structured method of response to noncompliance. This establishes a process that others can understand and thus recognize not only what is expected of them but also what they can expect as a response to their noncompliance.

Organizational security policies are also referred to as master security policies. An organization will have many policies, and they should be set up in a hierarchical manner. The organizational (master) security policy is at the highest level, with policies underneath it that address security issues specifically. These are referred to as issue-specific policies.

An *issue-specific policy*, also called a *functional policy*, addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues. For example, an organization may choose to have an e-mail security policy that outlines what management can and cannot do with employees' e-mail messages for monitoring purposes, that specifies which e-mail functionality employees can or cannot use, and that addresses specific privacy issues.

As a more specific example, an e-mail policy might state that management can read any employee's e-mail messages that reside on the mail server, but not when they reside on the user's workstation. The e-mail policy might also state that employees cannot use e-mail to share confidential information or pass inappropriate material and that they may be subject to monitoring of these actions. Before they use their e-mail clients, employees should be asked to confirm that they have read and understand the e-mail policy, either by signing a confirmation document or clicking Yes in a confirmation dialog box. The policy provides direction and structure for the staff by indicating what they can and cannot do. It informs the users of the expectations of their actions, and it provides liability protection in case an employee cries "foul" for any reason dealing with e-mail use.



EXAM TIP A policy needs to be technology and solution independent. It must outline the goals and missions, but not tie the organization to specific ways of accomplishing them.

A common hierarchy of security policies is outlined here, which illustrates the relationship between the master policy and the issue-specific policies that support it:

Organizational policy:

- Acceptable use policy
- Risk management policy
- Vulnerability management policy
- Data protection policy
- Access control policy
- Business continuity policy
- Log aggregation and auditing policy
- Personnel security policy
- Physical security policy
- Secure application development policy
- Change control policy
- E-mail policy
- Incident response policy

A *system-specific policy* presents the management's decisions that are specific to the actual computers, networks, and applications. An organization may have a system-specific policy outlining how a database containing sensitive information should be protected, who can have access, and how auditing should take place. It may also have a system-specific policy outlining how laptops should be locked down and managed. This policy type is directed to one or a group of similar systems and outlines how they should be protected.

Policies are written in broad terms to cover many subjects in a general fashion. Much more granularity is needed to actually support the policy, and this happens with the use of procedures, standards, guidelines, and baselines. The policy provides the foundation. The procedures, standards, guidelines, and baselines provide the security framework. And the necessary security controls (administrative, technical, and physical) are used to fill in the framework to provide a full security program.

Standards

Standards refer to mandatory activities, actions, or rules. Standards describe specific requirements that allow us to meet our policy goals. They are unambiguous, detailed, and measurable. There should be no question as to whether a specific asset or action complies with a given standard.

Organizational security standards may specify how hardware and software products are to be used. They can also be used to indicate expected user behavior. They provide a

Types of Policies

Policies generally fall into one of the following categories:

- **Regulatory** This type of policy ensures that the organization is following standards set by specific industry regulations (HIPAA, GLBA, SOX, PCI DSS, etc.; see Chapter 3). It is very detailed and specific to a type of industry. It is used in financial institutions, healthcare facilities, public utilities, and other government-regulated industries.
- **Advisory** This type of policy strongly advises employees as to which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical or financial information.
- **Informative** This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one that teaches individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations.

means to ensure that specific technologies, applications, parameters, and procedures are implemented in a uniform (standardized) manner across the organization. Organizational standards may require that all employees use a specific smart card as their access control token, that its certificate expire after 12 months, and that it be locked after three unsuccessful attempts to enter a personal identification number (PIN). These rules are compulsory within a company, and if they are going to be effective, they must be enforced.

An organization may have an issue-specific data classification policy that states "All confidential data must be properly protected." It would need a supporting data protection standard outlining how this protection should be implemented and followed, as in "Confidential information must be protected with AES256 at rest and in transit."

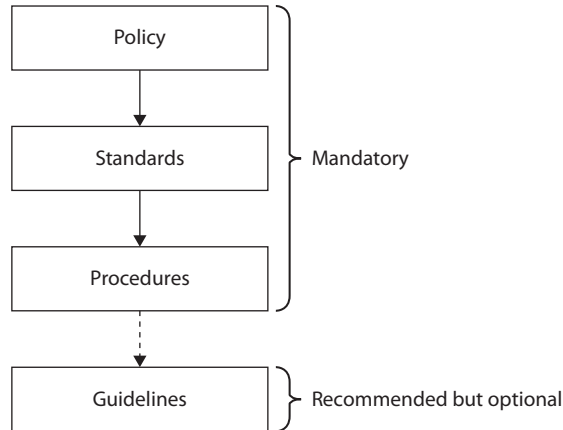
Tactical and strategic goals are different. A strategic goal can be viewed as the ultimate endpoint, while tactical goals are the steps necessary to achieve it. As shown in Figure 1-3, standards, guidelines, and procedures are the tactical tools used to achieve and support the directives in the security policy, which is considered the strategic goal.



EXAM TIP The term *standard* has more than one meaning in our industry. Internal documentation that lays out rules that must be followed is a standard. But sometimes, best practices, as in the ISO/IEC 27000 series, are referred to as standards because they were developed by a standards body. And as we will see later, we have specific technologic standards, as in IEEE 802.11. You need to understand the context of how this term is used. The CISSP exam will not try and trick you on this word; just know that the industry uses it in several different ways.

Figure 1-3

Policies are implemented through standards, procedures, and guidelines.



Baselines

The term *baseline* refers to a point in time that is used as a comparison for future changes. Once risks have been mitigated and security put in place, a baseline is formally reviewed and agreed upon, after which all further comparisons and development are measured against it. A baseline results in a consistent reference point.

Let's say that your doctor has told you that you're overweight due to your diet of donuts, pizza, and soda. (This is very frustrating to you because the supplement company's TV commercial said you could eat whatever you wanted and just take their very expensive pills every day and lose weight.) The doctor tells you that you need to exercise each day and elevate your heart rate to double its normal rate for 30 minutes twice a day. How do you know when you are at double your heart rate? You find out your baseline (regular heart rate) by using a heart rate monitor or going old school and manually taking your pulse with a stopwatch. So you start at your baseline and continue to exercise until you have doubled your heart rate or die, whichever comes first.

Baselines are also used to define the minimum level of protection required. In security, specific baselines can be defined per system type, which indicates the necessary settings and the level of protection being provided. For example, a company may stipulate that all accounting systems must meet an Evaluation Assurance Level (EAL) 4 baseline. This means that only systems that have gone through the Common Criteria process and achieved this rating can be used in this department. Once the systems are properly configured, this is the necessary baseline. When new software is installed, when patches or upgrades are applied to existing software, or when other changes to the system take place, there is a good chance the system may no longer be providing its necessary minimum level of protection (its baseline). Security personnel must assess the systems as changes take place and ensure that the baseline level of security is always being met. If a technician installs a patch on a system and does not ensure the baseline is still being met, there could be new vulnerabilities introduced into the system that will allow attackers easy access to the network.



NOTE Baselines that are not technology oriented should be created and enforced within organizations as well. For example, a company can mandate that while in the facility all employees must have a badge with a picture ID in view at all times. It can also state that visitors must sign in at a front desk and be escorted while in the facility. If these rules are followed, then this creates a baseline of protection.

Guidelines

Guidelines are recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply. They can also be used as a recommended way to achieve specific standards when those do apply. Guidelines can deal with the methodologies of technology, personnel, or physical security. Life is full of gray areas, and guidelines can be used as a reference during those times. Whereas standards are specific mandatory rules, guidelines are general approaches that provide the necessary flexibility for unforeseen circumstances.

A policy might state that access to confidential data must be audited. A supporting guideline could further explain that audits should contain sufficient information to allow for reconciliation with prior reviews. Supporting procedures would outline the necessary steps to configure, implement, and maintain this type of auditing.

Procedures

Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal. The steps can apply to users, IT staff, operations staff, security members, and others who may need to carry out specific tasks. Many organizations have written procedures on how to install operating systems, configure security mechanisms, implement access control lists, set up new user accounts, assign computer privileges, audit activities, destroy material, report incidents, and much more.

Procedures are considered the lowest level in the documentation chain because they are closest to the computers and users (compared to policies) and provide detailed steps for configuration and installation issues.

Procedures spell out how the policy, standards, and guidelines will actually be implemented in an operating environment. If a policy states that all individuals who access confidential information must be properly authenticated, the supporting procedures will explain the steps for this to happen by defining the access criteria for authorization, how access control mechanisms are implemented and configured, and how access activities are audited. If a policy states that backups should be performed, then the procedures will define the detailed steps necessary to perform the backup, the timelines of backups, the storage of backup media, and so on. Procedures should be detailed enough to be both understandable and useful to a diverse group of individuals.

Implementation

To tie these items together, let's walk through an implementation example. A corporation's security *policy* indicates that confidential information should be properly protected.

It states the issue in very broad and general terms. A supporting *standard* mandates that all customer information held in databases must be encrypted with the Advanced Encryption Standard (AES) algorithm while it is stored and that it cannot be transmitted over the Internet unless IPSec encryption technology is used. The standard indicates what type of protection is required and provides another level of granularity and explanation. The supporting *procedures* explain exactly how to implement the AES and IPSec technologies, and the *guidelines* cover how to handle cases when data is accidentally corrupted or compromised during transmission. Once the software and devices are configured as outlined in the procedures, this is considered the *baseline* that must always be maintained. All of these work together to provide a company with a security structure.

Unfortunately, security policies, standards, procedures, baselines, and guidelines often are written because an auditor instructed a company to document these items, but then they are placed on a file server and are not shared, explained, or used. To be useful, they must be put into action. Employees aren't going to follow the rules if they don't know the rules exist. Security policies and the items that support them not only must be developed but must also be implemented and enforced.

To be effective, employees need to know about security issues within these documents; therefore, the policies and their supporting counterparts need visibility. Awareness training, manuals, presentations, newsletters, and screen banners can achieve this visibility. It must be clear that the directives came from senior management and that the full management staff supports these policies. Employees must understand what is expected of them in their actions, behaviors, accountability, and performance.

Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is expected of them and the consequences of noncompliance can come down to a liability issue. For example, if a company fires an employee because he was downloading pornographic material to the company's computer, the employee may take the company to court and win if the employee can prove he was not properly informed of what was considered acceptable and unacceptable use of company property and what the consequences were. Security awareness training is covered later in this chapter, but personnel security is much broader than that.

Personnel Security

Although society has evolved to be extremely dependent upon technology in the workplace, people are still the key ingredient to a successful company. But in security circles, people are often the weakest link. Either accidentally through mistakes or lack of training, or intentionally through fraud and malicious intent, personnel cause more serious and hard-to-detect security issues than hacker attacks, outside espionage, or equipment failure. Although the future actions of individuals cannot be predicted, it is possible to minimize the risks by implementing preventive measures. These include hiring the most qualified individuals, performing background checks, using detailed job descriptions, providing necessary training, enforcing strict access controls, and terminating individuals in a way that protects all parties involved.

Several items can be put into place to reduce the possibilities of fraud, sabotage, misuse of information, theft, and other security compromises. *Separation of duties (SoD)* makes sure that one individual cannot complete a critical task by herself. In the movies, when a submarine captain needs to launch a nuclear missile to blow up the enemy and save (or end) civilization as we know it, the launch usually requires two codes to be entered into the launching mechanism by two different senior crewmembers. This is an example of separation of duties, and it ensures that the captain cannot complete such an important and terrifying task all by himself.

Separation of duties is a security control that can reduce the potential for fraud. For example, an employee cannot complete a critical financial transaction by herself. She will need to have her supervisor's approval before the transaction can be completed. There is usually a third person involved who verifies that this procedure was followed.

In an organization that practices separation of duties, collusion must take place for fraud to be committed. *Collusion* means that at least two people are working together to cause some type of destruction or fraud. In our example, the employee and her supervisor must be participating in the fraudulent activity to make it happen. Even if this were to happen, the third person who reviewed the transaction would provide a way to detect this collusion early enough (hopefully) to stop the transaction.

Two variations of separation of duties are *split knowledge* and *dual control*. In both cases, two or more individuals are authorized and required to perform a duty or task. In the case of split knowledge, no one person knows or has all the details to perform a task. For example, two managers might be required to open a bank vault, with each only knowing part of the combination. In the case of dual control, two individuals are again authorized to perform a task, but both must be available and active in their participation to complete the task or mission. For example, two officers must perform an identical key-turn in a nuclear missile submarine, each out of reach of the other, to launch a missile. The control here is that no one person has the capability of launching a missile, because they cannot reach to turn both keys at the same time.

These are examples of what is generally known as an *m of n control*, which is a control that requires a certain number of agents (*m*) out of a pool of authorized agents (*n*) to complete an operation. This type of control can also be called *quorum authentication*, because it requires the collaboration of a certain number of individuals (the quorum). In the bank vault example, if there were five managers authorized to open the vault and two were required to actually open it, this would be a 2 of 5 control, since $m = 2$ and $n = 5$. You don't want to make *n* too big because that increases the odds that two individuals could secretly conspire to do something harmful. On the other hand, you would not want *m* and *n* to have the same value, since the loss of any one individual would render the vault unopenable!

Job rotation (rotation of assignments) is an administrative detective control that can be put into place to uncover fraudulent activities. No one person should stay in one position for a long time because they may end up having too much control over a segment of the business. Such total control could result in fraud or the misuse of resources. Employees should be moved into different roles with the idea that they may be able to detect suspicious activity carried out by the previous employee filling that position. This type of control is commonly implemented in financial institutions.

Employees in sensitive areas should be forced to take their vacations, which is known as a *mandatory vacation*. While they are on vacation, other individuals fill their positions and thus can usually detect any fraudulent errors or activities. Two of the many ways to detect fraud or inappropriate activities would be the discovery of activity on someone's user account while they're supposed to be away on vacation, or if a specific problem stopped while someone was away and not active on the network. These anomalies are worthy of investigation. Employees who carry out fraudulent activities commonly do not take vacations because they do not want anyone to figure out what they are doing behind the scenes. This is why they must periodically be required to be away from the organization for a period of time, usually two weeks. Placing someone on administrative leave during an investigation is also a form of mandatory vacation.

Candidate Screening and Hiring

The issues, policies, and procedures discussed in the previous section are important to consider in the daily operations of your organization's staff, but let's not get too far ahead of ourselves. Personnel security starts way before a staff member shows up for work. Hiring the right candidate for a position can have a significant impact on the organization's security.

Depending on the position to be filled, human resources should perform a level of candidate screening to ensure that the company hires the right individual for the right job. Each candidate's skills should be tested and evaluated, and the caliber and character of the individual should be examined. Joe might be the best programmer in the state, but if someone looks into his past and finds out he served prison time because he hacked into a bank, the hiring manager might not be so eager to bring Joe into the organization.

Human resources should contact candidates' references, review their military records, if applicable, verify their educational background, obtain their credit report, check out their publicly viewable social media presence, and, if necessary, require proof of a recently administered negative drug test. Many times, candidates are able to conceal important personal behaviors, which is why hiring practices now include scenario questions, personality tests, and observations of the individual, instead of just looking at a person's work history. When a person is hired, he is bringing his skills and whatever other baggage he carries. A company can reduce its headache pertaining to personnel by first conducting useful and careful hiring practices.

The goal is to hire the "right person" and not just hire a person for "right now." Employees represent an investment on the part of the organization, and by taking the time and hiring the right people for the jobs, the organization will be able to maximize its investment and achieve a better return. Many organizations place a lot of value on determining whether a candidate is a good "cultural" fit. This means that the person will blend well into the culture that already exists in the company. People who fit in are more likely to follow the existing norms, policies, and procedures.

A detailed background check can reveal some interesting information. Things like unexplained gaps in employment history, the validity and actual status of professional certifications, criminal records, driving records, job titles that have been misrepresented, credit histories, unfriendly terminations, appearances on suspected terrorist watch lists, and even real reasons for having left previous jobs can all be determined through the use

of background checks. This has real benefit to the employer and the organization because it serves as the first line of defense for the organization against being attacked from within. Any negative information found in these areas could be indicators of potential problems that the candidate could create for the company at a later date if hired. Take the credit report, for instance. On the surface, the candidate's credit standing may seem to be personal information that the organization doesn't need to know about, but if the report indicates the potential employee has a poor credit standing and a history of financial problems, your organization certainly won't want to place that person in charge of its accounting, or even the petty cash.

Ultimately, the goal of performing background checks is to achieve several different things for the organization at the same time:

- Mitigate risk
- Lower hiring and training costs and the turnover rate for employees
- Protect customers and employees from someone who could potentially conduct malicious and dishonest actions that could harm the organization, its employees, and its customers as well as the general public

In many cases, it is also harder to go back and conduct background checks after the individual has been hired and is working, because there will need to be a specific cause or reason for conducting this kind of investigation. If any employee moves to a position of greater security sensitivity or potential risk, a follow-up investigation should be considered.

Possible background check criteria could include

- National identification number trace
- Criminal check
- Sexual offender registry check
- Employment verification
- Education verification
- Professional reference verification
- Immigration check
- Professional license/certification verification
- Credit report
- Drug screening

Employment Agreements and Policies

Congratulations! Your organization found the right candidate who passed its screening with flying colors and accepted the offer of employment. Now what? Depending on the jurisdiction in which your organization is located, it may be legally required as an employer to enter into a contract or other agreement with the candidate in order for the

hiring action to be official. Whether or not this is a requirement for your organization, it is almost always a good idea to put this employment agreement in writing and ensure that it is signed by both parties. If you are a hiring manager, you should always follow the guidance provided by your human resources and legal teams, but it is useful to be aware of how this all works.

One of the key elements of an employment agreement is a reference to the policies that are applicable to employees in their new roles. Again, depending on where you are in the world, some policies (typically those dealing with safety and welfare) may be required to be included or referenced in the agreement. At a minimum, the employment agreement should include language pointing to the employee manual or other repository of policies for your organization. The point is that every new hire should sign an agreement stating that they are aware of the policies with which they must comply as a condition of employment. This becomes particularly helpful if there are any allegations of misconduct later on. For example, absent a signed employment agreement, if an employee deliberately (or even maliciously) accesses a computer or files that she shouldn't, she could claim she was never told it was wrong and get off the hook. According to the Federal Bureau of Investigation (FBI) manual on prosecuting computer crimes, "it is relatively easy to prove that a defendant had only limited authority to access a computer in cases where the defendant's access was limited by restrictions that were memorialized in writing, such as terms of service, a computer access policy, a website notice, or an employment agreement or similar contract."

Another important element of an employment agreement is the establishment of a probationary period. This is a period of time during which it is relatively easy to fire the new employee for misconduct or just failing to live up to expectations. Depending on the laws in your jurisdiction, it could be difficult to get rid of an employee even if it's obvious they are not working out. A probationary period could be helpful should you decide that your new hire is not as good as you thought.

Onboarding, Transfers, and Termination Processes

Onboarding is the process of turning a candidate into a trusted employee who is able to perform all assigned duties. Having a structured and well-documented onboarding process not only will make the new employee feel valued and welcome but will also ensure that your organization doesn't forget any security tasks. Though the specific steps will vary by organization, the following are some that are pretty universal:

- The new employee attends all required security awareness training.
- The new employee must read all security policies, be given an opportunity to have any questions about the policies answered, and sign a statement indicating they understand and will comply with the policies.
- The new employee is issued all appropriate identification badges, keys, and access tokens pursuant to their assigned roles.
- The IT department creates all necessary accounts for the new employee, who signs into the systems and sets their passwords (or changes any temporary passwords).

Organizations should develop *nondisclosure agreements (NDAs)* and require them to be signed by new employees to protect the organization and its sensitive information. NDAs typically specify what is considered sensitive information, how it should be protected, when it can be shared with others, and how long these obligations last after the employee (or the agreement) is terminated.

One of the most overlooked issues in personnel security is what happens when an employee's role within the organization changes. This could be a promotion (or demotion), assumption of new additional roles, loss of old roles, transfer to another business unit, or perhaps the result of a total restructuring of a business unit. Typically, what happens is that whatever old authorizations the employee had are never taken away, but new ones are added. Over time, employees who've been transferred or reassigned could accumulate a very extensive set of authorizations on information systems that they no longer need to access. IT and security staff need to be involved in transfers and role changes so that they can determine what policies apply and which permissions should be added, left in place, or removed. The goal is to ensure that every staff member has the permissions they need to do their jobs, and not a single one more.

Unfortunately, sometimes organizations have to terminate employees. Because terminations can happen for a variety of reasons, and terminated people have different reactions, companies should have a specific set of procedures to follow with every termination to ensure that their security posture isn't undermined in the process. For example:

- The employee must leave the facility immediately under the supervision of a manager or security guard.
- The employee must surrender any identification badges or keys, be asked to complete an exit interview, and return company supplies.
- That user's accounts and passwords must be disabled or changed immediately.

These actions may seem harsh when they actually take place, but too many companies have been hurt by vengeful employees who have retaliated against the companies after their positions were revoked for one reason or another. If an employee is disgruntled in any way or the termination is unfriendly, that employee's accounts must be disabled right away, and all passwords on all systems must be changed.

Practical Tips on Terminations

Without previous arrangement, an employee cannot be compelled to complete an exit interview, despite the huge value to the company of conducting such interviews. Neither can an employee be compelled to return company property, as a practical matter, if he or she simply chooses not to. The best way to motivate departing employees to comply is to ensure that any severance package they may be eligible for is contingent upon completion of these tasks, and that means having them agree to such conditions up-front, as part of their employment agreement.

Vendors, Consultants, and Contractors

Many companies today could not perform their business functions without the services of an assortment of vendors, consultants, and contractors who have different levels of access to the companies' facilities and information systems. From the janitorial staff who have physical access to virtually any area of a facility to the outsourced software developers in a different country who could introduce (willingly or otherwise) vulnerabilities (or even backdoors) to the companies' most sensitive systems, the risks associated with vendors, consultants, and contractors can be significant if left unmitigated.

There are a number of approaches to dealing with third parties in your environment from an information security standpoint. One approach is to enter into service agreements that require contractors to use security controls that are at least as stringent as your organization's security controls, *and* to prove it. The service agreement could include specific requirements for security controls or leverage existing standards such as the International Organization for Standardization (ISO) 27001 certification (which we discuss in Chapter 4). Either way, the agreement must specify a way to verify compliance with the contractual obligations and clearly state the penalties for failing to meet those obligations.

Another approach to dealing with third parties is to assume that vendors, consultants, and contractors are untrusted and place strict controls around every aspect of their performance. For example, you could require that janitors be escorted by designated employees and that outsourced developers work on virtual desktop infrastructure under the control of your organization. You could also require that highly sensitive assets (e.g., proprietary algorithms, trade secrets, and customer data) be off limits to these third parties. This approach will likely reduce certain risks but may not be ideal for building partnerships or engendering mutual trust.

There is no single best way to deal with the security issues inherent in working with third parties. As with every aspect of personnel security, you should work in close coordination with your business units, human resources staff, and legal counsel. Coordinating with legal counsel is particularly critical, because your organization's liability may (and often does) extend to the actions and inactions of your vendors, consultants, and contractors. For example, if your organization's network is breached because one of your contractors violated policies and that breach resulted in customers' PII being stolen and causing them financial losses, your company could be liable for their damages. This is known as *downstream liability*.

Compliance Policies

There are many forms of liability that may pertain to your organization. Your organization may be subject to external regulations that require special attention and compliance from a security standpoint. Examples are healthcare providers in the United States, who fall under the Healthcare Insurance Portability and Accountability Act (HIPAA); companies that handle payment card information, which must follow the Payment Card Industry Data Security Standard (PCI DSS); and organizations that handle personal information of citizens of the European Union, which fall under the General Data Protection Regulation (GDPR). Many more examples exist, but the point is that if your organization is regulated,

then your personnel security practices must comply with these regulations. As a security leader, you should know which regulations apply to your organization and how security policies, including personnel security ones, work to ensure regulatory compliance.

Privacy Policies

Even if your organization doesn't fall under GDPR or any of the myriad of similar privacy regulations and laws, there are good reasons for you to ensure that your organization has a privacy policy and that your information security practices are aligned with it. For example, suppose you have a policy that allows employees to privately check personal webmail during their breaks, and you also have a policy of decrypting and inspecting all web traffic on your networks to ensure no adversaries are using encryption to sneak around your security controls. These two policies could be in conflict with each other. Worse yet, an employee could sue for violation of privacy if his e-mail messages are intercepted and read by your security team.

Security Awareness, Education, and Training Programs

Even if you develop security policies that protect organizational assets and are aligned with all relevant laws and regulations, it is all for naught if nobody knows what they are expected to do. For an organization to achieve the desired results of its security program, it must communicate the what, how, and why of security to its employees. Security awareness training should be comprehensive, tailored for specific groups, and organization-wide. It should repeat the most important messages in different formats; be kept up to date; be entertaining, positive, and humorous; be simple to understand; and—most important—be supported by senior management. Management must allocate the resources for this activity and enforce its attendance within the organization.

The goal is for each employee to understand the importance of security to the company as a whole and to each individual. Expected responsibilities and acceptable behaviors must be clarified, and noncompliance repercussions, which could range from a warning to dismissal, must be explained before being invoked. Security awareness training can modify employees' behavior and attitude toward security. This can best be achieved through a formalized process of security awareness training.

Degree or Certification?

Some roles within the organization need hands-on experience and skill, meaning that the hiring manager should be looking for specific industry certifications. Some positions require more of a holistic and foundational understanding of concepts or a business background, and in those cases a degree may be required. Table 1-3 provides more information on the differences between awareness, training, and education.

	Awareness	Training	Education
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Learning objective	Recognition and retention	Skill	Understanding
Example teaching method	Media: Videos Newsletters Posters CBT Social engineering testing	Practical Instruction: Lecture and/or demo Case study Hands-on practice	Theoretical Instruction: Seminar and discussion Reading and study Research
Test measure	True/False, multiple choice (identify learning)	Problem solving—i.e., recognition and resolution (apply learning)	Essay (interpret learning)
Impact timeframe	Short-term	Intermediate	Long-term

Table 1-3 Aspects of Awareness, Training, and Education

Methods and Techniques to Present Awareness and Training

Because security is a topic that can span many different aspects of an organization, it can be difficult to communicate the correct information to the right individuals. By using a formalized process for security awareness training, you can establish a method that will provide you with the best results for making sure security requirements are presented to the right people in an organization. This way you can make sure everyone understands what is outlined in the organization's security program, why it is important, and how it fits into the individual's role in the organization. The higher levels of training typically are more general and deal with broader concepts and goals, and as the training moves down to specific jobs and tasks, it becomes more situation specific as it directly applies to certain positions within the company.

A security awareness program is typically created for at least three types of audiences: management, staff, and technical employees. Each type of awareness training must be geared toward the individual audience to ensure each group understands its particular responsibilities, liabilities, and expectations. If technical security training were given to senior management, their eyes would glaze over as soon as protocols and firewalls were mentioned. On the flip side, if legal ramifications, company liability issues pertaining to protecting data, and shareholders' expectations were discussed with the IT group, they would quickly turn to their smartphone and start tweeting, browsing the Internet, or texting their friends.

Members of senior management would benefit the most from a short, focused security awareness orientation that discusses corporate assets and financial gains and losses pertaining to security. They need to know how stock prices can be negatively affected by compromises, understand possible threats and their outcomes, and know why security

must be integrated into the environment the same way as other business processes. Because members of management must lead the rest of the company in support of security, they must gain the right mindset about its importance.

Middle management would benefit from a more detailed explanation of the policies, procedures, standards, and guidelines and how they map to the individual departments for which each middle manager is responsible. Middle managers should be taught why their support for their specific departments is critical and what their level of responsibility is for ensuring that employees practice safe computing activities. They should also be shown how the consequences of noncompliance by individuals who report to them can affect the company as a whole and how they, as managers, may have to answer for such indiscretions.

Staff training, which typically involves the largest portion of an organization, should provide plenty of examples of specific behaviors that are expected, recommended, and forbidden. This is an opportunity to show how alert users can be sensors providing early warning of attacks, which can dramatically improve the security posture of any organization. This can be accomplished by training the staff to recognize and report the sorts of attacks they are likely to face. Conversely, it is important to also show the consequences, organizational and personal, of being careless or violating policies and procedures.

The technical departments must receive a different presentation that aligns more to their daily tasks. They should receive a more in-depth training to discuss technical configurations, incident handling, and how to recognize different types of security compromises.

Perhaps no other topic is more important or better illustrates the need to communicate security issues differently to each of these three audiences than the topic of social engineering. *Social engineering* is the deliberate manipulation of a person or group of persons to persuade them to do something they otherwise wouldn't or shouldn't. In a security context, this typically means getting a member of the organization to violate a security policy or procedure or to help an attacker compromise a system. The most common form of social engineering is *phishing*, which is the use of e-mail messages to perform social engineering. While all employees should know that they should not click on links or open attachments in e-mail messages if they don't recognize the sender, executives, managers, and end users should be presented the problem in a different light.

Regardless of how the training is presented, it is usually best to have each employee sign a document indicating they have heard and understand all the security topics discussed and that they also understand the ramifications of noncompliance. This reinforces the policies' importance to the employee and also provides evidence down the road if the employee claims they were never told of these expectations. Awareness training should happen during the hiring process and at least annually after that. Attendance of training should also be integrated into employment performance reports.

Various methods should be employed to reinforce the concepts of security awareness. Things like screen banners, employee handbooks, and even posters can be used as ways to remind employees about their duties and the necessities of good security practices. But there are other ways to drive employee engagement. For example, *gamification* is the application of elements of game play to other activities such as security awareness training. By some accounts, gamification can improve employees' skill retention by 40 percent. Another approach is to leverage employees who are not formally part of the

security program and yet have the skills and aptitudes that make them security advocates within their own business units. These individuals can be identified and deliberately nurtured to act as conduits between business units and the security program. They can become *security champions*, which are members of an organization that, though their job descriptions do not include security, inform and encourage the adoption of security practices within their own teams.

Periodic Content Reviews

The only constant in life is change, so it should come as no surprise that after we develop the curricula and materials for security awareness training, we have to keep them up to date by conducting periodic content reviews. It is essential that this be a deliberate process and not done in an ad hoc manner. One way to do this is to schedule refreshes at specific intervals like semi-annually or yearly and assign the task to an individual owner. This person would work with a team to review and update the plan and materials but is ultimately responsible for keeping the training up to date.

Another approach is to have content reviews be triggered by other events. For example, reviews can be required whenever any of the following occur:

- A security policy is added, changed, or discontinued
- A major incident (or pattern of smaller incidents) occurs that could've been avoided or mitigated through better security awareness
- A major new threat is discovered
- A major change is made to the information systems or security architecture
- An assessment of the training program shows deficiencies

Program Effectiveness Evaluation

Many organizations treat security awareness training as a “check in the box” activity that is done simply to satisfy a requirement. The reality, however, is that effective training has both objectives (why we do it) and outcomes (what people can do after participating in it). The objectives are usually derived from senior-level policies or directives and drive the development of outcomes, which in turn drive the content and methods of delivery. For example, if the objective is reducing the incidence of successful phishing attacks, then it would be appropriate to pursue an outcome of having end users be able to detect a phishing e-mail. Both the objective and the outcome are measurable, which makes it easier to answer the question “is this working?”

We can evaluate whether the security training program is effective in improving an organization's security posture by simply measuring things before the training and then after it. Continuing the earlier example, we could keep track of the number of successful phishing attacks and see what happens to that number after the training has been conducted. This would be an assessment of the objective. We could also take trained and untrained users and test their ability to detect phishing e-mails. We would expect the trained users to fare better at this task, which would test the outcome. If we see that the number of phishing

attacks remains unchanged (or worse, grows) or that the users are no better at detecting phishing e-mails after the training, then maybe the program is not effective.

When assessing the effectiveness of a training program, it is very important to analyze the data and not jump to conclusions. In the phishing example, there are many possible explanations for the lack of improvement. Maybe the adversaries are sending more-sophisticated messages that are harder to detect. Similarly, the results could simply show that the users just don't care and will continue to click links and open attachments until the consequences become negative enough for them. The point is to consider the root causes of the measurements when assessing the training.

Professional Ethics

Security awareness and training, of course, build on the notion that there are right ways and wrong ways in which to behave. This is the crux of ethics, which can be based on many different issues and foundations. Ethics can be relative to different situations and interpreted differently from individual to individual. Therefore, they are often a topic of debate. However, some ethics are less controversial than others, and these types of ethics are easier to expect of all people.

An interesting relationship exists between law and ethics. Most often, laws are based on ethics and are put in place to ensure that others act in an ethical way. However, laws do not apply to everything—that is when ethics should kick in. Some things may not be illegal, but that does not necessarily mean they are ethical.

Certain common ethical fallacies are used by many in the computing world to justify unethical acts. They exist because people look at issues differently and interpret (or misinterpret) rules and laws that have been put into place. The following are examples of these ethical fallacies:

- Hackers only want to learn and improve their skills. Many of them are not making a profit off of their deeds; therefore, their activities should not be seen as illegal or unethical.
- The First Amendment protects and provides the right for U.S. citizens to write viruses.
- Information should be shared freely and openly; therefore, sharing confidential information and trade secrets should be legal and ethical.
- Hacking does not actually hurt anyone.

(ISC)² Code of Professional Ethics

(ISC)² requires all certified system security professionals to commit to fully supporting its Code of Ethics. If a CISSP intentionally or knowingly violates this Code of Ethics, he or she may be subject to a peer review panel, which will decide whether the certification should be revoked.

The (ISC)² Code of Ethics for the CISSP is listed on the (ISC)² site at <https://www.isc2.org/Ethics>. The following list is an overview, but each CISSP candidate should read

the full version and understand the Code of Ethics before attempting this exam. The code's preamble makes it clear that "[t]he safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior." It goes on to provide four canons for CISSPs:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

Organizational Code of Ethics

More regulations are requiring organizations to have an ethical statement and potentially an ethical program in place. The ethical program is to serve as the "tone at the top," which means that the executives need to ensure not only that their employees are acting ethically but also that they themselves are following their own rules. The main goal is to ensure that the motto "succeed by any means necessary" is not the spoken or unspoken culture of a work environment. Certain structures can be put into place that provide a breeding ground for unethical behavior. If the CEO gets more in salary based on stock prices, then she may find ways to artificially inflate stock prices, which can directly hurt the investors and shareholders of the company. If managers can only be promoted based on the amount of sales they bring in, these numbers may be fudged and not represent reality. If an employee can only get a bonus if a low budget is maintained, he might be willing to take shortcuts that could hurt company customer service or product development. Although ethics seem like things that float around in the ether and make us feel good to talk about, they have to be actually implemented in the real corporate world through proper business processes and management styles.

The Computer Ethics Institute

The *Computer Ethics Institute* is a nonprofit organization that works to help advance technology by ethical means.

The Computer Ethics Institute has developed its own Ten Commandments of Computer Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.

7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Chapter Review

This chapter laid out some of the fundamental principles of cybersecurity: the meaning of security, how it is governed, and the means by which it is implemented in an enterprise. It then focused on the most important aspect of security: people. They are the most important asset to any organization and can also be the greatest champions, or underminers, of cybersecurity. The difference lies in who we hire, what roles we assign to them, and how we train them. Bring the right people into the right seats and train them well and you'll have a robust security posture. Do otherwise at your own peril.

Our collective goal in information systems security boils down to ensuring the availability, integrity, and confidentiality of our information in an environment rich in influencers. These include organizational goals, assets, laws, regulations, privacy, threats, and, of course, people. Each of these was discussed in some detail in this chapter. Along the way, we also covered tangible ways in which we can link security to each of the influencers. As CISSPs we must be skilled in creating these linkages, as we are trusted to be able to apply the right solution to any security problem.

Quick Review

- The objectives of security are to provide confidentiality, integrity, availability, authenticity, and nonrepudiation.
- Confidentiality means keeping unauthorized entities (be they people or processes) from gaining access to information assets.
- Integrity means that an asset is free from unauthorized alterations.
- Availability protection ensures reliability and timely access to data and resources to authorized individuals.
- Authenticity protections ensure we can trust that something comes from its claimed source.
- Nonrepudiation, which is closely related to authenticity, means that someone cannot disavow being the source of a given action.
- A vulnerability is a weakness in a system that allows a threat source to compromise its security.

- A threat is any potential danger that is associated with the exploitation of a vulnerability.
- A threat source (or threat agent, or threat actor) is any entity that can exploit a vulnerability.
- A risk is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact.
- A control, or countermeasure, is put into place to mitigate (reduce) the potential risk.
- Security governance is a framework that provides oversight, accountability, and compliance.
- An information security management system (ISMS) is a collection of policies, procedures, baselines, and standards that an organization puts in place to make sure that its security efforts are aligned with business needs, streamlined, and effective and that no security controls are missing.
- An enterprise security architecture implements an information security strategy and consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally.
- An enterprise security architecture should tie in strategic alignment, business enablement, process enhancement, and security effectiveness.
- Security governance is a framework that supports the security goals of an organization being set and expressed by senior management, communicated throughout the different levels of the organization, and consistently applied and assessed.
- Senior management always carries the ultimate responsibility for the organization.
- A security policy is a statement by management dictating the role security plays in the organization.
- Standards are documents that describe specific requirements that are compulsory in nature and support the organization's security policies.
- A baseline is a minimum level of security.
- Guidelines are recommendations and general approaches that provide advice and flexibility.
- Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal.
- Job rotation and mandatory vacations are administrative security controls that can help detect fraud.
- Separation of duties ensures no single person has total control over a critical activity or task.
- Split knowledge and dual control are two variations of separation of duties.

- Social engineering is an attack carried out to manipulate a person into providing sensitive data to an unauthorized individual.
- Security awareness training should be comprehensive, tailored for specific groups, and organization-wide.
- Gamification is the application of elements of game play to other activities such as security awareness training.
- Security champions, which are members of an organization that, though their job descriptions do not include security, inform and encourage the adoption of security practices within their own teams.
- Professional ethics codify the right ways for a group of people to behave.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. Which factor is the most important item when it comes to ensuring security is successful in an organization?
 - A. Senior management support
 - B. Effective controls and implementation methods
 - C. Updated and relevant security policies and procedures
 - D. Security awareness by all employees

Use the following scenario to answer Questions 2–4. Todd is a new security manager and has the responsibility of implementing personnel security controls within the financial institution where he works. Todd knows that many employees do not fully understand how their actions can put the institution at risk; thus, he needs to develop a security awareness program. He has determined that the bank tellers need to get a supervisory override when customers have checks over \$3,500 that need to be cashed. He has also uncovered that some employees have stayed in their specific positions within the company for over three years. Todd would like to be able to investigate some of the activities of bank personnel to see if any fraudulent activities have taken place. Todd is already ensuring that two people must use separate keys at the same time to open the bank vault.

2. Todd documents several fraud opportunities that the employees have at the financial institution so that management understands these risks and allocates the funds and resources for his suggested solutions. Which of the following best describes the control Todd should put into place to be able to carry out fraudulent investigation activity?
 - A. Separation of duties
 - B. Job rotation
 - C. Mandatory vacations
 - D. Split knowledge
3. If the financial institution wants to ensure that fraud cannot happen successfully unless collusion occurs, what should Todd put into place?
 - A. Separation of duties
 - B. Job rotation
 - C. Social engineering
 - D. Split knowledge
4. Todd wants to be able to prevent fraud from taking place, but he knows that some people may get around the types of controls he puts into place. In those situations he wants to be able to identify when an employee is doing something suspicious. Which of the following incorrectly describes what Todd is implementing in this scenario and what those specific controls provide?
 - A. Separation of duties, by ensuring that a supervisor must approve the cashing of a check over \$3,500. This is an administrative control that provides preventive protection for Todd's organization.
 - B. Job rotation, by ensuring that one employee only stays in one position for up to three months at a time. This is an administrative control that provides detective capabilities.
 - C. Security awareness training, which can also emphasize enforcement.
 - D. Dual control, which is an administrative detective control that can ensure that two employees must carry out a task simultaneously.
5. Which term denotes a potential cause of an unwanted incident, which may result in harm to a system or organization?
 - A. Vulnerability
 - B. Exploit
 - C. Threat
 - D. Attacker

6. A CISSP candidate signs an ethics statement prior to taking the CISSP examination. Which of the following would be a violation of the (ISC)² Code of Ethics that could cause the candidate to lose his or her certification?
 - A. E-mailing information or comments about the exam to other CISSP candidates
 - B. Submitting comments on the questions of the exam to (ISC)²
 - C. Submitting comments to the board of directors regarding the test and content of the class
 - D. Conducting a presentation about the CISSP certification and what the certification means
7. You want to ensure that your organization's finance department, and only the finance department, has access to the organization's bank statements. Which of the security properties would be most important?
 - A. Confidentiality
 - B. Integrity
 - C. Availability
 - D. Both A and C
8. You want to make use of the OpenOffice productivity software suite mandatory across your organization. In what type of document would you codify this?
 - A. Policy
 - B. Standard
 - C. Guideline
 - D. Procedure
9. For an enterprise security architecture to be successful in its development and implementation, which of the following items is not essential?
 - A. Strategic alignment
 - B. Security guidelines
 - C. Business enablement
 - D. Process enhancement
10. Which of the following practices is likeliest to mitigate risks when considering a candidate for hiring?
 - A. Security awareness training
 - B. Nondisclosure agreement (NDA)
 - C. Background checks
 - D. Organizational ethics

Answers

1. **A.** Without senior management's support, a security program will not receive the necessary attention, funds, resources, and enforcement capabilities.
2. **C.** Mandatory vacation is an administrative detective control that allows for an organization to investigate an employee's daily business activities to uncover any potential fraud that may be taking place. The employee should be forced to be away from the organization for a two-week period, and another person should be put into that role. The idea is that the person who was rotated into that position may be able to detect suspicious activities.
3. **A.** Separation of duties is an administrative control that is put into place to ensure that one person cannot carry out a critical task by himself. If a person were able to carry out a critical task alone, this could put the organization at risk. Collusion is when two or more people come together to carry out fraud. So if a task was split between two people, they would have to carry out collusion (working together) to complete that one task and carry out fraud.
4. **D.** Dual control is an administrative preventive control. It ensures that two people must carry out a task at the same time, as in two people having separate keys when opening the vault. It is not a detective control. Notice that the question asks what Todd is *not* doing. Remember that on the exam you need to choose the *best* answer. In many situations you will not like the question or the corresponding answers on the CISSP exam, so prepare yourself. The questions can be tricky, which is one reason why the exam itself is so difficult.
5. **C.** The question provides the definition of a threat. The term attacker (option D) could be used to describe a threat agent that is, in turn, a threat, but use of this term is much more restrictive. The best answer is a threat.
6. **A.** A CISSP candidate and a CISSP holder should never discuss with others what was on the exam. This degrades the usefulness of the exam to be used as a tool to test someone's true security knowledge. If this type of activity is uncovered, the person could be stripped of their CISSP certification because this would violate the terms of the NDA into which the candidate enters prior to taking the test. Violating an NDA is a violation of the ethics canon that requires CISSPs to act honorably, honestly, justly, responsibly, and legally.
7. **D.** Confidentiality is ensuring that unauthorized parties (i.e., anyone other than finance department employees) cannot access protected assets. Availability is ensuring that authorized entities (i.e., finance) maintain access to assets. In this case, both confidentiality and availability are important to satisfy the requirements as stated.
8. **B.** Standards describe mandatory activities, actions, or rules. A policy is intended to be strategic, so it would not be the right document. A procedure describes the manner in which something must be done, which is much broader than is needed to make using a particular software suite mandatory across your organization. Finally, guidelines are recommended but optional practices.

- 9. **B.** Security guidelines are optional recommendations on issues that are not covered by mandatory policies, standards, or procedures. A successful enterprise security architecture is aligned with the organization's strategy, enables its business, and enhances (rather than hinders) its business processes.
- 10. **C.** The best way to reduce risk is to conduct background checks before you offer employment to a candidate. This ensures you are hiring someone whose past has been examined for any obviously disqualifying (or problematic) issues. The next step would be to sign an employment agreement that would include an NDA, followed by onboarding, which would include security awareness training and indoctrination into the organizational code of ethics.

Risk Management

This chapter presents the following:

- Risk management (assessing risks, responding to risks, monitoring risks)
- Supply chain risk management
- Business continuity

A ship in harbor is safe, but that is not what ships are built for.

—William G.T. Shedd

We next turn our attention to the concept that should underlie every decision made when defending our information systems: risk. Risk is so important to understand as a cybersecurity professional that we not only cover it in detail in this chapter (one of the longest in the book) but also return to it time and again in the rest of the book. We start off narrowly by focusing on the vulnerabilities in our organizations and the threats that would exploit them to cause us harm. That sets the stage for an in-depth discussion of the main components of risk management: framing, assessing, responding to, and monitoring risks. We pay particular attention to supply chain risks, since these represent a big problem to which many organizations pay little or no attention. Finally, we'll talk about business continuity because it is so closely linked to risk management. We'll talk about disaster recovery, a closely related concept, in later chapters.

Risk Management Concepts

Risk in the context of security is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact. *Risk management (RM)* is the process of identifying and assessing risk, reducing it to an acceptable level, and ensuring it remains at that level. There is no such thing as a 100-percent-secure environment. Every environment has vulnerabilities and threats. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Risks to an organization come in different forms, and they are not all computer related. As we saw in Chapter 1, when a company acquires another company, it takes on a lot of risk in the hope that this move will increase its market base, productivity,

and profitability. If a company increases its product line, this can add overhead, increase the need for personnel and storage facilities, require more funding for different materials, and maybe increase insurance premiums and the expense of marketing campaigns. The risk is that this added overhead might not be matched in sales; thus, profitability will be reduced or not accomplished.

When we look at information security, note that an organization needs to be aware of several types of risk and address them properly. The following items touch on the major categories:

- **Physical damage** Fire, water, vandalism, power loss, and natural disasters
- **Human interaction** Accidental or intentional action or inaction that can disrupt productivity
- **Equipment malfunction** Failure of systems and peripheral devices
- **Inside and outside attacks** Hacking, cracking, and attacking
- **Misuse of data** Sharing trade secrets, fraud, espionage, and theft
- **Loss of data** Intentional or unintentional loss of information to unauthorized parties
- **Application error** Computation errors, input errors, and software defects

Threats must be identified, classified by category, and evaluated to calculate their damage potential to the organization. Real risk is hard to measure, but prioritizing the potential risks in the order of which ones must be addressed first is obtainable.

Holistic Risk Management

Who really understands risk management? Unfortunately, the answer to this question is that not enough people inside or outside of the security profession really get it. Even though information security is big business today, the focus all too often is on applications, devices, viruses, and hacking. Although these items all must be considered and weighed in risk management processes, they should be considered pieces of the overall security puzzle, not the main focus of risk management.

Security is a business issue, but businesses operate to make money, not just to be secure. A business is concerned with security only if potential risks threaten its bottom line, which they can in many ways, such as through the loss of reputation and customer base after a database of credit card numbers is compromised; through the loss of thousands of dollars in operational expenses from a new computer worm; through the loss of proprietary information as a result of successful company espionage attempts; through the loss of confidential information from a successful social engineering attack; and so on. It is critical that security professionals understand these individual threats, but it is more important that they understand how to calculate the risk of these threats and map them to business drivers.

To properly manage risk within an organization, you have to look at it holistically. Risk, after all, exists within a context. The U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk*, defines three tiers to risk management:

- **Organization view (Tier 1)** Concerned with risk to the organization as a whole, which means it frames the rest of the conversation and sets important parameters such as the risk tolerance level.
- **Mission/business process view (Tier 2)** Deals with the risk to the major functions of the organization, such as defining the criticality of the information flows between the organization and its partners or customers.
- **Information systems view (Tier 3)** Addresses risk from an information systems perspective. Though this is where we will focus our discussion, it is important to understand that it exists within the context of (and must be consistent with) other, more encompassing risk management efforts.

These tiers are dependent on each other, as shown in Figure 2-1. Risk management starts with decisions made at the organization tier, which flow down to the other two tiers. Feedback on the effects of these decisions flows back up the hierarchy to inform the next set of decisions to be made. Carrying out risk management properly means that you have a holistic understanding of your organization, the threats it faces, the countermeasures that can be put into place to deal with those threats, and continuous monitoring to ensure the acceptable risk level is being met on an ongoing basis.

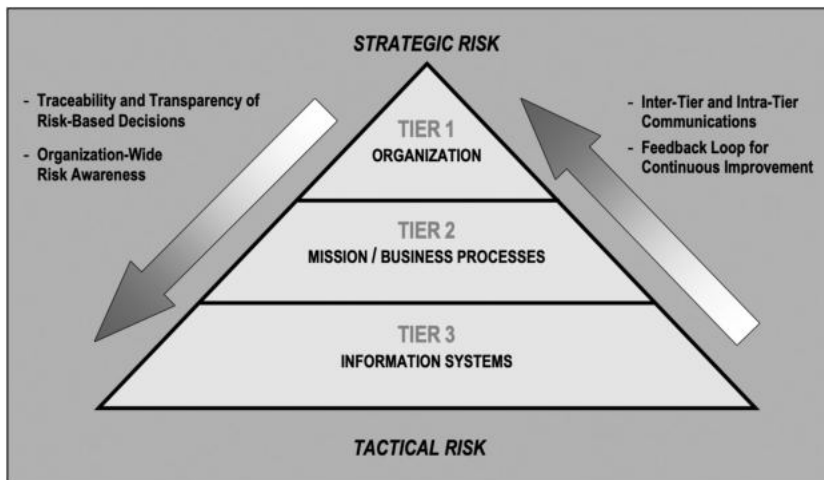


Figure 2-1 The three tiers of risk management (Source: NIST SP 800-39)

Information Systems Risk Management Policy

Proper risk management requires a strong commitment from senior leaders, a documented process that supports the organization's mission, an information systems risk management (ISRM) policy, and a delegated ISRM team. The ISRM policy should be a subset of the organization's overall risk management policy (*risks to an organization include more than just information security issues*) and should be mapped to the organizational security policies. The ISRM policy should address the following items:

- The objectives of the ISRM team
- The level of risk the organization will accept and what is considered an acceptable level of risk
- Formal processes of risk identification
- The connection between the ISRM policy and the organization's strategic planning processes
- Responsibilities that fall under ISRM and the roles to fulfill them
- The mapping of risk to internal controls
- The approach toward changing staff behaviors and resource allocation in response to risk analysis
- The mapping of risks to performance targets and budgets
- Key metrics and performance indicators to monitor the effectiveness of controls

The ISRM policy provides the foundation and direction for the organization's security risk management processes and procedures and should address all issues of information security. It should provide direction on how the ISRM team communicates information on the organization's risks to senior management and how to properly execute management's decisions on risk mitigation tasks.

The Risk Management Team

Each organization is different in its size, security posture, threat profile, and security budget. One organization may have one individual responsible for ISRM or a team that works in a coordinated manner. The overall goal of the team is to ensure that the organization is protected in the most cost-effective manner. This goal can be accomplished only if the following components are in place:

- An established risk acceptance level provided by senior management
- Documented risk assessment processes and procedures
- Procedures for identifying and mitigating risks
- Appropriate resource and fund allocation from senior management
- Security awareness training for all staff members associated with information assets
- The ability to establish improvement (or risk mitigation) teams in specific areas when necessary

- The mapping of legal and regulation compliancy requirements to control and implement requirements
- The development of metrics and performance indicators so as to measure and manage various types of risks
- The ability to identify and assess new risks as the environment and organization change
- The integration of ISRM and the organization's change control process to ensure that changes do not introduce new vulnerabilities

Obviously, this list is a lot more than just buying a new shiny firewall and calling the organization safe.

The ISRM team, in most cases, is not made up of employees with the dedicated task of risk management. It consists of people who already have a full-time job in the organization and are now tasked with something else. Thus, senior management support is necessary so proper resource allocation can take place.

Of course, all teams need a leader, and ISRM is no different. One individual should be singled out to run this rodeo and, in larger organizations, this person should be spending 50 to 70 percent of their time in this role. Management must dedicate funds to making sure this person receives the necessary training and risk analysis tools to ensure it is a successful endeavor.

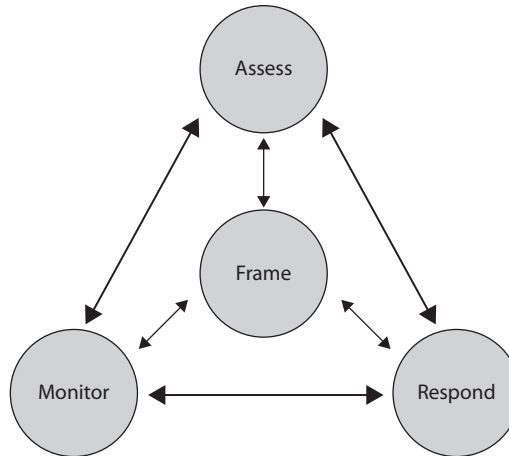
The Risk Management Process

By now you should believe that risk management is critical to the long-term security (and even success) of your organization. But how do you get this done? NIST SP 800-39 describes four interrelated components that comprise the risk management process. These are shown in Figure 2-2. Let's consider each of these components briefly now, since they will nicely frame the remainder of our discussion of risk management.

- **Frame risk** Risk framing defines the context within which all other risk activities take place. What are our assumptions and constraints? What are the organizational priorities? What is the risk tolerance of senior management?
- **Assess risk** Before we can take any action to mitigate risk, we have to assess it. This is perhaps the most critical aspect of the process, and one that we will discuss at length. If your risk assessment is spot-on, then the rest of the process becomes pretty straightforward.
- **Respond to risk** By now, we've done our homework. We know what we should, must, and can't do (from the framing component), and we know what we're up against in terms of threats, vulnerabilities, and attacks (from the assess component). Responding to the risk becomes a matter of matching our limited resources with our prioritized set of controls. Not only are we mitigating significant risk, but, more importantly, we can tell our bosses what risk we can't do anything about because we're out of resources.

Figure 2-2

The components of the risk management process



- **Monitor risk** No matter how diligent we've been so far, we probably missed something. If not, then the environment likely changed (perhaps a new threat source emerged or a new system brought new vulnerabilities). In order to stay one step ahead of the bad guys, we need to continuously monitor the effectiveness of our controls against the risks for which we designed them.

You will notice that our discussion of risk so far has dealt heavily with the whole framing process. In the preceding sections, we've talked about the organization (top to bottom), the policies, and the team. The next step is to assess the risk, and what better way to start than by understanding threats and the vulnerabilities they might exploit.

Overview of Vulnerabilities and Threats

To focus our efforts on the likely (and push aside the less likely) risks to our organizations, we need to consider what it is that we have that someone (or something) else may be able to take, degrade, disrupt, or destroy. As we will see later (in the section "Assessing Risks"), inventorying and categorizing our information systems is a critical early step in the process. For the purpose of modeling the threat, we are particularly interested in the vulnerabilities inherent in our systems that could lead to the compromise of their confidentiality, integrity, or availability. We then ask the question, "Who would want to exploit this vulnerability, and why?" This leads us to a deliberate study of our potential adversaries, their motivations, and their capabilities. Finally, we determine whether a given threat source has the means to exploit one or more vulnerabilities in order to attack our assets.



NOTE We will discuss threat modeling in detail in Chapter 9.

Vulnerabilities

Everything built by humans is vulnerable to something. Our information systems, in particular, are riddled with vulnerabilities even in the best-defended cases. One need only read news accounts of the compromise of the highly protected and classified systems of defense contractors and even governments to see that this universal principle is true. To properly analyze vulnerabilities, it is useful to recall that information systems consist of information, processes, and people that are typically, but not always, interacting with computer systems. Since we discuss computer system vulnerabilities in detail in Chapter 6, we will briefly discuss the other three components here.

Information In almost every case, the information at the core of our information systems is the most valuable asset to a potential adversary. Information within a computer information system (CIS) is represented as data. This information may be stored (data at rest), transported between parts of our system (data in transit), or actively being used by the system (data in use). In each of its three states, the information exhibits different vulnerabilities, as listed in the following examples:

- **Data at rest** Data is copied to a thumb drive and given to unauthorized parties by an insider, thus compromising its confidentiality.
- **Data in transit** Data is modified by an external actor intercepting it on the network and then relaying the altered version (known as a man-in-the-middle or MitM attack), thus compromising its integrity.
- **Data in use** Data is deleted by a malicious process exploiting a “time-of-check to time-of-use” (TOC/TOU) or “race condition” vulnerability, thus compromising its availability.

Processes Most organizations implement standardized processes to ensure the consistency and efficiency of their services and products. It turns out, however, that efficiency is pretty easy to hack. Consider the case of shipping containers. Someone wants to ship something from point A to point B, say a container of bananas from Brazil to Belgium. Once the shipping order is placed and the destination entered, that information flows from the farm to a truck carrier, to the seaport of origin to the ocean carrier, to the destination seaport, to another truck carrier, and finally to its destination at some distribution center in Antwerp. In most cases, nobody pays a lot of attention to the address once it is entered. But what if an attacker knew this and changed the address while the shipment was at sea? The attacker could have the shipment show up at a different destination and even control the arrival time. This technique has actually been used by drug and weapons smuggling gangs to get their “bananas” to where they need them.

This sort of attack is known as *business process compromise (BPC)* and is commonly targeted at the financial sector, where transaction amounts, deposit accounts, or other parameters are changed to funnel money to the attackers’ pockets. Since business processes are almost always instantiated in software as part of a CIS, process vulnerabilities can be thought of as a specific kind of software vulnerability. As security professionals, however,

it is important that we take a broader view of the issue and think about the business processes that are implemented in our software systems.

People Many security experts consider humans to be the weakest link in the security chain. Whether or not you agree with this, it is important to consider the specific vulnerabilities that people present in a system. Though there are many ways to exploit the human in the loop, there are three that correspond to the bulk of the attacks, summarized briefly here:

- **Social engineering** This is the process of getting a person to violate a security procedure or policy, and usually involves human interaction or e-mail/text messages.
- **Social networks** The prevalence of social network use provides potential attackers with a wealth of information that can be leveraged directly (e.g., blackmail) or indirectly (e.g., crafting an e-mail with a link that is likely to be clicked) to exploit people.
- **Passwords** Weak passwords can be cracked in milliseconds using rainbow tables and are very susceptible to dictionary or brute-force attacks. Even strong passwords are vulnerable if they are reused across sites and systems.

Threats

As you identify the vulnerabilities that are inherent to your organization and its systems, it is important to also identify the sources that could attack them. The International Organization for Standardization and the International Electrotechnical Commission in their joint ISO/IEC standard 27000 define a *threat* as a “potential cause of an unwanted incident, which can result in harm to a system or organization.” While this may sound somewhat vague, it is important to include the full breadth of possibilities. When a threat is one or more humans, we typically use the term *threat actor* or *threat agent*. Let’s start with the most obvious: malicious humans.

Cybercriminals Cybercriminals are the most common threat actors encountered by individuals and organizations. Most cybercriminals are motivated by greed, but some just enjoy breaking things. Their skills run the gamut, from so-called *script kiddies* with just a basic grasp of hacking (but access to someone else’s scripts or tools) to sophisticated cybercrime gangs who develop and sometimes sell or rent their services and tools to others. Cybercrime is the fastest-growing sector of criminal activity in many countries.

One of the factors that makes cybercrime so pervasive is that every connected device is a target. Some devices are immediately monetizable, such as your personal smartphone or home computer containing credentials, payment card information, and access to your financial institutions. Other targets provide bigger payouts, such as the finance systems in your place of work. Even devices that are not, by themselves, easily monetizable can be hijacked and joined into a botnet to spread malware, conduct distributed denial-of-service (DDoS) attacks, or serve as staging bases from which to attack other targets.

Nation-State Actors Whereas cybercriminals tend to cast a wide net in an effort to maximize their profits, nation-state actors (or simply *state actors*) are very selective in

who they target. They use advanced capabilities to compromise systems and establish a persistent presence to allow them to collect intelligence (e.g., sensitive data, intellectual property, etc.) for extended periods. After their presence is established, state actors may use prepositioned assets to trigger devastating effects in response to world events. Though their main motivations tend to be espionage and gaining persistent access to critical infrastructure, some state actors maintain good relations with cybercrime groups in their own country, mostly for the purposes of plausible deniability. By collaborating with these criminals, state actors can make it look as if an attack against another nation was a crime and not an act of war. At least one country is known to use its national offensive cyber capabilities for financial profit, stealing millions of dollars all over the world.

Many security professionals consider state actors a threat mostly to government organizations, critical infrastructure like power plants, and anyone with sophisticated research and development capabilities. In reality, however, these actors can and do target other organizations, typically to use them as a springboard into their ultimate targets. So, even if you work for a small company that seems uninteresting to a foreign nation, you could find your company in a state actor's crosshairs.

Hacktivists Hacktivists use cyberattacks to effect political or social change. The term covers a diverse ecosystem, encompassing individuals and groups of various skillsets and capabilities. Hacktivists' preferred objectives are highly visible to the public or yield information that, when made public, aims to embarrass government entities or undermine public trust in them.

Internal Actors Internal actors are people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems. Broadly speaking, there are two types of insider threats: negligent and malicious. A negligent insider is one who fails to exercise due care, which puts their organization at risk. Sometimes, these individuals knowingly violate policies or disregard procedures, but they are not doing so out of malicious intent. For example, an employee could disregard a policy requiring visitors to be escorted at all times because someone shows up wearing the uniform of a telecommunications company and claiming to be on site to fix an outage. This insider trusts the visitor, which puts the organization at risk, particularly if that person is an impostor.

The second type of insider threat is characterized by malicious intent. Malicious insiders use the knowledge they have about their organization either for their own advantage (e.g., to commit fraud) or to directly cause harm (e.g., by deleting sensitive files). While some malicious insiders plan their criminal activity while they are employees in good standing, others are triggered by impending termination actions. Knowing (or suspecting) that they're about to be fired, they may attempt to steal sensitive data (such as customer contacts or design documents) before their access is revoked. Other malicious insiders may be angry and plant malware or destroy assets in an act of revenge. This insider threat highlights the need for the "zero trust" secure design principle (discussed in Chapter 9). It is also a really good reason to practice the termination processes discussed in Chapter 1.

In the wake of the massive leak of classified data attributed to Edward Snowden in 2012, there's been increased emphasis on techniques and procedures for identifying and mitigating the insider threat source. While the deliberate insider dominates the news, it is important to note that the accidental insider can be just as dangerous, particularly if they fall into one of the vulnerability classes described in the preceding section.

Nature Finally, the nonhuman threat source can be just as important as the ones we've previously discussed. Hurricane Katrina in 2005 and the Tohoku earthquake and tsunami in 2011 serve as reminders that natural events can be more destructive than any human attack. They also force the information systems security professional to consider threats that fall way outside the norm. Though it is easier and, in many cases, cheaper to address likelier natural events such as a water main break or a fire in a facility, one should always look for opportunities to leverage countermeasures that protect against both mild and extreme events for small price differentials.

Identifying Threats and Vulnerabilities

Earlier, it was stated that the definition of a risk is the probability of a threat exploiting a vulnerability to cause harm to an asset and the resulting business impact. Many types of threat actors can take advantage of several types of vulnerabilities, resulting in a variety of specific threats, as outlined in Table 2-1, which represents only a sampling of the risks many organizations should address in their risk management programs.

Other types of threats can arise in an environment that are much harder to identify than those listed in Table 2-1. These other threats have to do with application and user errors. If an application uses several complex equations to produce results, the threat can be difficult to discover and isolate if these equations are incorrect or if the application is using inputted data incorrectly. This can result in *illogical processing* and *cascading errors* as invalid results are passed on to another process. These types of problems can lie within application code and are very hard to identify.

Threat Actor	Can Exploit This Vulnerability	To Cause This Effect
Cybercriminal	Lack of antimalware software	Ransomed data
Nation-state actor	Password reuse in privileged accounts	Unauthorized access to confidential information
Negligent user	Misconfigured parameter in the operating system	Loss of availability due to a system malfunction
Fire	Lack of fire extinguishers	Facility and computer loss or damage, and possibly loss of life
Malicious insider	Poor termination procedures	Deletion of business-critical information
Hacktivist	Poorly written web application	Website defacement
Burglar	Lack of security guard	Breaking windows and stealing computers and devices

Table 2-1 Relationship of Threats and Vulnerabilities

User errors, whether intentional or accidental, are easier to identify by monitoring and auditing users' activities. Audits and reviews must be conducted to discover if employees are inputting values incorrectly into programs, misusing technology, or modifying data in an inappropriate manner.

After the ISRM team has identified the vulnerabilities and associated threats, it must investigate the ramifications of any of those vulnerabilities being exploited. Risks have *loss potential*, meaning that the organization could lose assets or revenues if a threat agent actually exploited a vulnerability. The loss may be corrupted data, destruction of systems and/or the facility, unauthorized disclosure of confidential information, a reduction in employee productivity, and so on. When performing a risk assessment, the team also must look at *delayed loss* when assessing the damages that can occur. Delayed loss is secondary in nature and takes place well after a vulnerability is exploited. Delayed loss may include damage to the organization's reputation, loss of market share, accrued late penalties, civil suits, the delayed collection of funds from customers, resources required to reimage other compromised systems, and so forth.

For example, if a company's web servers are attacked and taken offline, the immediate damage (loss potential) could be data corruption, the man-hours necessary to place the servers back online, and the replacement of any code or components required. The company could lose revenue if it usually accepts orders and payments via its website. If getting the web servers fixed and back online takes a full day, the company could lose a lot more sales and profits. If getting the web servers fixed and back online takes a full week, the company could lose enough sales and profits to not be able to pay other bills and expenses. This would be a delayed loss. If the company's customers lose confidence in it because of this activity, the company could lose business for months or years. This is a more extreme case of delayed loss.

These types of issues make the process of properly quantifying losses that specific threats could cause more complex, but they must be taken into consideration to ensure reality is represented in this type of analysis.

Assessing Risks

A *risk assessment*, which is really a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls. After parts of a risk assessment are carried out, the results are analyzed. *Risk analysis* is a detailed examination of the components of risk that is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. It is easy to apply too much security, not enough security, or the wrong security controls and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps organizations prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in a sensible manner.



EXAM TIP The terms risk assessment and risk analysis, depending on who you ask, can mean the same thing, or one must follow the other, or one is a subpart of the other. Here, we treat risk assessment as the broader effort, which is reinforced by specific risk analysis tasks as needed. This is how you should think of it for the CISSP exam.

Risk analysis has four main goals:

- Identify assets and their value to the organization.
- Determine the likelihood that a threat exploits a vulnerability.
- Determine the business impact of these potential threats.
- Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Risk analysis provides a *cost/benefit comparison*, which compares the annualized cost of controls to the potential cost of loss. A control, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the control itself. This means that if a facility is worth \$100,000, it does not make sense to spend \$150,000 trying to protect it.

It is important to figure out what you are *supposed* to be doing before you dig right in and start working. Anyone who has worked on a project without a properly defined scope can attest to the truth of this statement. Before an assessment is started, the team must carry out *project sizing* to understand what assets and threats should be evaluated. Most assessments are focused on physical security, technology security, or personnel security. Trying to assess all of them at the same time can be quite an undertaking.

One of the risk assessment team's tasks is to create a report that details the asset valuations. Senior management should review and accept the list and use these values to determine the scope of the risk management project. If management determines at this early stage that some assets are not important, the risk assessment team should not spend additional time or resources evaluating those assets. During discussions with management, everyone involved must have a firm understanding of the value of the security CIA triad—confidentiality, integrity, and availability—and how it directly relates to business needs.

Management should outline the scope of the assessment, which most likely will be dictated by organizational compliance requirements as well as budgetary constraints. Many projects have run out of funds, and consequently stopped, because proper project sizing was not conducted at the onset of the project. Don't let this happen to you.

A risk assessment helps integrate the security program objectives with the organization's business objectives and requirements. The more the business and security objectives are in alignment, the more successful both will be. The assessment also helps the organization draft a proper budget for a security program and its constituent security components. Once an organization knows how much its assets are worth and the possible threats those assets are exposed to, it can make intelligent decisions about how much money to spend protecting those assets.

A risk assessment must be supported and directed by senior management if it is to be successful. Management must define the purpose and scope of the effort, appoint a team to carry out the assessment, and allocate the necessary time and funds to conduct it. It is essential for senior management to review the outcome of the risk assessment and to act on its findings. After all, what good is it to go through all the trouble of a risk assessment and *not* react to its findings? Unfortunately, this does happen all too often.

Asset Valuation

To understand possible losses and how much we may want to invest in preventing them, we must understand the value of an asset that could be impacted by a threat. The value placed on information is relative to the parties involved, what work was required to develop it, how much it costs to maintain, what damage would result if it were lost or destroyed, how much money enemies would pay for it, and what liability penalties could be endured. If an organization does not know the value of the information and the other assets it is trying to protect, it does not know how much money and time it should spend on protecting them. If the calculated value of your company's secret formula is x , then the total cost of protecting it should be some value less than x . Knowing the value of our information allows us to make quantitative cost/benefit comparisons as we manage our risks.

The preceding logic applies not only to assessing the value of *information* and protecting it but also to assessing the value of the organization's other assets, such as facilities, systems, and even intangibles like the value of the brand, and protecting them. The value of the organization's facilities must be assessed, along with all printers, workstations, servers, peripheral devices, supplies, and employees. You do not know how much is in danger of being lost if you don't know what you have and what it is worth in the first place.

The actual value of an asset is determined by the importance it has to the organization as a whole. The value of an asset should reflect all identifiable costs that would arise if the asset were actually impaired. If a server cost \$4,000 to purchase, this value should not be input as the value of the asset in a risk assessment. Rather, the cost of replacing or repairing it, the loss of productivity, and the value of any data that may be corrupted or lost must be accounted for to properly capture the amount the organization would lose if the server were to fail for one reason or another.

The following issues should be considered when assigning values to assets:

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Price others are willing to pay for the asset
- Cost to replace the asset if lost
- Operational and production activities affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness and role of the asset in the organization
- Impact of the asset's loss on the organization's brand or reputation

Understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. A very important question is how much it could cost the organization to *not* protect the asset.

Determining the value of assets may be useful to an organization for a variety of reasons, including the following:

- To perform effective cost/benefit analyses
- To select specific countermeasures and safeguards
- To determine the level of insurance coverage to purchase
- To understand what exactly is at risk
- To comply with legal and regulatory requirements

Assets may be tangible (computers, facilities, supplies) or intangible (reputation, data, intellectual property). It is usually harder to quantify the values of intangible assets, which may change over time. How do you put a monetary value on a company's reputation? This is not always an easy question to answer, but it is important to be able to do so.

Risk Assessment Teams

Each organization has different departments, and each department has its own functionality, resources, tasks, and quirks. For the most effective risk assessment, an organization must build a risk assessment team that includes individuals from many or all departments to ensure that all of the threats are identified and addressed. The team members may be part of management, application programmers, IT staff, systems integrators, and operational managers—indeed, any key personnel from key areas of the organization. This mix is necessary because if the team comprises only individuals from the IT department, it may not understand, for example, the types of threats the accounting department faces with data integrity issues, or how the organization as a whole would be affected if the accounting department's data files were wiped out by an accidental or intentional act.

Asking the Right Questions

When looking at risk, it's good to keep several questions in mind. Raising these questions helps ensure that the risk assessment team and senior management know what is important. Team members must ask the following:

- What event could occur (threat event)?
- What could be the potential impact (risk)?
- How often could it happen (frequency)?
- What level of confidence do we have in the answers to the first three questions (certainty)?

A lot of this information is gathered through internal surveys, interviews, or workshops. Viewing threats with these questions in mind helps the team focus on the tasks at hand and assists in making the decisions more accurate and relevant.

Or, as another example, the IT staff may not understand all the risks the employees in the warehouse would face if a natural disaster were to hit, or what it would mean to their productivity and how it would affect the organization overall. If the risk assessment team is unable to include members from various departments, it should, at the very least, make sure to interview people in each department so it fully understands and can quantify all threats.

The risk assessment team must also include people who understand the processes that are part of their individual departments, meaning individuals who are at the right levels of each department. This is a difficult task, since managers sometimes delegate any sort of risk assessment task to lower levels within the department. However, the people who work at these lower levels may not have adequate knowledge and understanding of the processes that the risk assessment team may need to deal with.

Methodologies for Risk Assessment

The industry has different standardized methodologies for carrying out risk assessments. Each of the individual methodologies has the same basic core components (identify vulnerabilities, associate threats, calculate risk values), but each has a specific focus. Keep in mind that the methodologies have a lot of overlapping similarities because each one has the specific goal of identifying things that could hurt the organization (vulnerabilities and threats) so that those things can be addressed (risk reduced). What make these methodologies different from each other are their unique approaches and focuses.

If you need to deploy an organization-wide risk management program and integrate it into your security program, you should follow the OCTAVE method. If you need to focus just on IT security risks during your assessment, you can follow NIST SP 800-30. If you have a limited budget and need to carry out a focused assessment on an individual system or process, you can follow the Facilitated Risk Analysis Process. If you really want to dig into the details of how a security flaw within a specific system could cause negative ramifications, you could use Failure Modes and Effect Analysis or fault tree analysis.

NIST SP 800-30

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, is specific to information systems threats and how they relate to information security risks. It lays out the following steps:

1. Prepare for the assessment.
2. Conduct the assessment:
 - a. Identify threat sources and events.
 - b. Identify vulnerabilities and predisposing conditions.
 - c. Determine likelihood of occurrence.
 - d. Determine magnitude of impact.
 - e. Determine risk.
3. Communicate results.
4. Maintain assessment.

The NIST risk management methodology is mainly focused on computer systems and IT security issues. It does not explicitly cover larger organizational threat types, as in succession planning, environmental issues, or how security risks associate to business risks. It is a methodology that focuses on the operational components of an enterprise, not necessarily the higher strategic level.

FRAP

Facilitated Risk Analysis Process (FRAP) is a second type of risk assessment methodology. The crux of this qualitative methodology is to focus only on the systems that really need assessing, to reduce costs and time obligations. FRAP stresses prescreening activities so that the risk assessment steps are only carried out on the item(s) that needs it the most. FRAP is intended to be used to analyze one system, application, or business process at a time. Data is gathered and threats to business operations are prioritized based upon their criticality. The risk assessment team documents the controls that need to be put into place to reduce the identified risks along with action plans for control implementation efforts.

This methodology does not support the idea of calculating exploitation probability numbers or annualized loss expectancy values. The criticalities of the risks are determined by the team members' experience. The author of this methodology (Thomas Peltier) believes that trying to use mathematical formulas for the calculation of risk is too confusing and time consuming. The goal is to keep the scope of the assessment small and the assessment processes simple to allow for efficiency and cost-effectiveness.

OCTAVE

The *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)* methodology was created by Carnegie Mellon University's Software Engineering Institute (SIE). OCTAVE is intended to be used in situations where people manage and direct the risk evaluation for information security within their organization. This places the people who work inside the organization in the power positions of being able to make the decisions regarding what is the best approach for evaluating the security of their organization. OCTAVE relies on the idea that the people working in these environments best understand what is needed and what kind of risks they are facing. The individuals who make up the risk assessment team go through rounds of facilitated workshops. The facilitator helps the team members understand the risk methodology and how to apply it to the vulnerabilities and threats identified within their specific business units. OCTAVE stresses a self-directed team approach.

The scope of an OCTAVE assessment is usually very wide compared to the more focused approach of FRAP. Where FRAP would be used to assess a system or application, OCTAVE would be used to assess all systems, applications, and business processes within the organization.

The OCTAVE methodology consists of the seven processes (or steps) listed here:

1. Identify enterprise knowledge.
2. Identify operational area knowledge.
3. Identify staff knowledge.

4. Establish security requirements.
5. Map high-priority information assets to information infrastructure.
6. Perform infrastructure vulnerability evaluation.
7. Conduct multidimensional risk analysis.
8. Develop protection strategy.

FMEA

Failure Modes and Effect Analysis (FMEA) is a method for determining functions, identifying functional failures, and assessing the causes of failure and their failure effects through a structured process. FMEA is commonly used in product development and operational environments. The goal is to identify where something is most likely going to break and either fix the flaws that could cause this issue or implement controls to reduce the impact of the break. For example, you might choose to carry out an FMEA on your organization's network to identify single points of failure. These single points of failure represent vulnerabilities that could directly affect the productivity of the network as a whole. You would use this structured approach to identify these issues (vulnerabilities), assess their criticality (risk), and identify the necessary controls that should be put into place (reduce risk).

The FMEA methodology uses failure modes (how something can break or fail) and effects analysis (impact of that break or failure). The application of this process to a chronic failure enables the determination of where exactly the failure is most likely to occur. Think of it as being able to look into the future and locate areas that have the potential for failure and then applying corrective measures to them before they do become actual liabilities.

By following a specific order of steps, the best results can be maximized for an FMEA:

1. Start with a block diagram of a system or control.
2. Consider what happens if each block of the diagram fails.
3. Draw up a table in which failures are paired with their effects and an evaluation of the effects.
4. Correct the design of the system, and adjust the table until the system is not known to have unacceptable problems.
5. Have several engineers review the Failure Modes and Effect Analysis.

Table 2-2 is an example of how an FMEA can be carried out and documented. Although most organizations will not have the resources to do this level of detailed work for every system and control, an organization can carry it out on critical functions and systems that can drastically affect the organization.

FMEA was first developed for systems engineering. Its purpose is to examine the potential failures in products and the processes involved with them. This approach proved to be successful and has been more recently adapted for use in evaluating risk management priorities and mitigating known threat vulnerabilities.

Prepared by:							
Approved by:							
Date:							
Revision:							
Item Identification	Function	Failure Mode	Failure Cause	Failure Effect on . . .			Failure Detection Method
				Component or Functional Assembly	Next Higher Assembly	System	
IPS application content filter	Inline perimeter protection	Fails to close	Traffic overload	Single point of failure Denial of service	IPS blocks ingress traffic stream	IPS is brought down	Health check status sent to console and e-mail to security administrator
Central antivirus signature update engine	Push updated signatures to all servers and workstations	Fails to provide adequate, timely protection against malware	Central server goes down	Individual node's antivirus software is not updated	Network is infected with malware	Central server can be infected and/or infect other systems	Heartbeat status check sent to central console, and e-mail to network administrator
Fire suppression water pipes	Suppress fire in building 1 in 5 zones	Fails to close	Water in pipes freezes	None	Building 1 has no suppression agent available	Fire suppression system pipes break	Suppression sensors tied directly into fire system central console
Etc.							

Table 2-2 How an FMEA Can Be Carried Out and Documented

FMEA is used in assurance risk management because of the level of detail, variables, and complexity that continues to rise as corporations understand risk at more granular levels. This methodical way of identifying potential pitfalls is coming into play more as the need for risk awareness—down to the tactical and operational levels—continues to expand.

Fault Tree Analysis

While FMEA is most useful as a survey method to identify major failure modes in a given system, the method is not as useful in discovering complex failure modes that may be involved in multiple systems or subsystems. A *fault tree analysis* usually proves to be a more useful approach to identifying failures that can take place within more complex environments and systems. First, an undesired effect is taken as the root or top event of a tree of logic. Then, each situation that has the potential to cause that effect is added to the tree as a series of logic expressions. Fault trees are then labeled with actual numbers pertaining to failure probabilities. This is typically done by using computer programs that can calculate the failure probabilities from a fault tree.

Figure 2-3 shows a simplistic fault tree and the different logic symbols used to represent what must take place for a specific fault event to occur.

When setting up the tree, you must accurately list all the threats or faults that can occur within a system. The branches of the tree can be divided into general categories, such as physical threats, network threats, software threats, Internet threats, and component failure threats. Then, once all possible general categories are in place, you can trim them and effectively prune from the tree the branches that won't apply to the system in question. In general, if a system is not connected to the Internet by any means, remove that general branch from the tree.

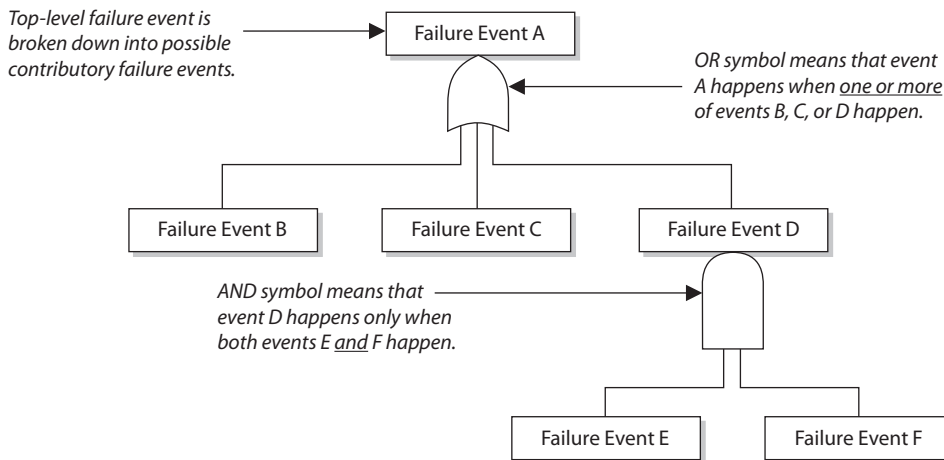


Figure 2-3 Fault tree and logic components

Some of the most common software failure events that can be explored through a fault tree analysis are the following:

- False alarms
- Insufficient error handling
- Sequencing or order
- Incorrect timing outputs
- Valid but unexpected outputs

Of course, because of the complexity of software and heterogeneous environments, this is a very small sample list.



EXAM TIP A risk assessment is used to gather data. A risk analysis examines the gathered data to produce results that can be acted upon.

Risk Analysis Approaches

So up to this point, we have accomplished the following items:

- Developed a risk management policy
- Developed a risk management team
- Identified organizational assets to be assessed
- Calculated the value of each asset
- Identified the vulnerabilities and threats that can affect the identified assets
- Chosen a risk assessment methodology that best fits our needs

The next thing we need to figure out is if our risk analysis approach should be quantitative or qualitative in nature. A *quantitative risk analysis* is used to assign monetary and numeric values to all elements of the risk analysis process. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks. It is more of a scientific or mathematical approach (objective) to risk analysis compared to qualitative. A *qualitative risk analysis* uses a “softer” approach to the data elements of a risk analysis. It does not quantify that data, which means that it does not assign numeric values to the data so that it can be used in equations. As an example, the results of a quantitative risk analysis could be that the organization is at risk of losing \$100,000 if a buffer overflow were exploited on a web server, \$25,000 if a database were compromised, and \$10,000 if a file server were compromised. A qualitative risk analysis would not present these findings in monetary values, but would assign ratings to the risks, as in Red, Yellow, and Green.

A quantitative analysis uses risk calculations that attempt to predict the level of monetary losses and the probability for each type of threat. Qualitative analysis does not

use calculations. Instead, it is more opinion and scenario based (subjective) and uses a rating system to relay the risk criticality levels.

Quantitative and qualitative approaches have their own pros and cons, and each applies more appropriately to some situations than others. An organization's management and risk analysis team, and the tools they decide to use, will determine which approach is best.

In the following sections we will dig into the depths of quantitative analysis and then revisit the qualitative approach. We will then compare and contrast their attributes.

Automated Risk Analysis Methods

Collecting all the necessary data that needs to be plugged into risk analysis equations and properly interpreting the results can be overwhelming if done manually. Several automated risk analysis tools on the market can make this task much less painful and, hopefully, more accurate. The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present to management.



EXAM TIP Remember that vulnerability assessments are different from risk assessments. A vulnerability assessment just finds the vulnerabilities (the holes). A risk assessment calculates the probability of the vulnerabilities being exploited and the associated business impact.

The objective of these tools is to reduce the manual effort of these tasks, perform calculations quickly, estimate future expected losses, and determine the effectiveness and benefits of the security countermeasures chosen. Most automatic risk analysis products port information into a database and run several types of scenarios with different parameters to give a panoramic view of what the outcome will be if different threats come to bear. For example, after such a tool has all the necessary information inputted, it can be rerun several times with different parameters to compute the potential outcome if a large fire were to take place; the potential losses if a virus were to damage 40 percent of the data on the main file server; how much the organization would lose if an attacker were to steal all the customer credit card information held in three databases; and so on. Running through the different risk possibilities gives an organization a more detailed understanding of which risks are more critical than others, and thus which ones to address first.

Steps of a Quantitative Risk Analysis

If we choose to carry out a quantitative risk analysis, then we are going to use mathematical equations for our data interpretation process. The most common equations used for this purpose are the *single loss expectancy (SLE)* and the *annualized loss expectancy (ALE)*. The SLE is a monetary value that is assigned to a single event that represents the organization's potential loss amount if a specific threat were to take place. The equation is laid out as follows:

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

The *exposure factor (EF)* represents the percentage of loss a realized threat could have on a certain asset. For example, if a data warehouse has the asset value of \$150,000, it can be estimated that if a fire were to occur, 25 percent of the warehouse would be damaged, in which case the SLE would be \$37,500:

$$\text{Asset Value } (\$150,000) \times \text{Exposure Factor } (25\%) = \$37,500$$

This tells us that the organization could potentially lose \$37,500 if a fire were to take place. But we need to know what our annual potential loss is, since we develop and use our security budgets on an annual basis. This is where the ALE equation comes into play. The ALE equation is as follows:

$$\text{SLE} \times \text{Annualized Rate of Occurrence (ARO)} = \text{ALE}$$

The *annualized rate of occurrence (ARO)* is the value that represents the estimated frequency of a specific threat taking place within a 12-month timeframe. The range can be from 0.0 (never) to 1.0 (once a year) to greater than 1 (several times a year), and anywhere in between. For example, if the probability of a fire taking place and damaging our data warehouse is once every 10 years, the ARO value is 0.1.

So, if a fire within an organization's data warehouse facility can cause \$37,500 in damages, and the frequency (or ARO) of a fire taking place has an ARO value of 0.1 (indicating once in 10 years), then the ALE value is \$3,750 ($\$37,500 \times 0.1 = \$3,750$).

The ALE value tells the organization that if it wants to put in controls to protect the asset (warehouse) from this threat (fire), it can sensibly spend \$3,750 or less per year to provide the necessary level of protection. Knowing the real possibility of a threat and how much damage, in monetary terms, the threat can cause is important in determining how much should be spent to try and protect against that threat in the first place. It would not make good business sense for the organization to spend more than \$3,750 per year to protect itself from this threat.

Clearly, this example is overly simplistic in focusing strictly on the structural losses. In the real world, we should include other related impacts such as loss of revenue due to the disruption, potential fines if the fire was caused by a violation of local fire codes, and injuries to employees that would require medical care. The number of factors to consider can be pretty large and, to some of us, not obvious. This is why you want to have a diverse risk assessment team that can think of all the myriad impacts that a simple event might have.

Uncertainty

In risk analysis, uncertainty refers to the degree to which you lack confidence in an estimate. This is expressed as a percentage, from 0 to 100 percent. If you have a 30 percent confidence level in something, then it could be said you have a 70 percent uncertainty level. Capturing the degree of uncertainty when carrying out a risk analysis is important, because it indicates the level of confidence the team and management should have in the resulting figures.

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
Facility	Fire	\$230,000	0.1	\$23,000
Trade secret	Stolen	\$40,000	0.01	\$400
File server	Failed	\$11,500	0.1	\$1,150
Business data	Ransomware	\$283,000	0.1	\$28,300
Customer credit card info	Stolen	\$300,000	3.0	\$900,000

Table 2-3 Breaking Down How SLE and ALE Values Are Used

Now that we have all these numbers, what do we do with them? Let’s look at the example in Table 2-3, which shows the outcome of a quantitative risk analysis. With this data, the organization can make intelligent decisions on what threats must be addressed first because of the severity of the threat, the likelihood of it happening, and how much could be lost if the threat were realized. The organization now also knows how much money it should spend to protect against each threat. This will result in good business decisions, instead of just buying protection here and there without a clear understanding of the big picture. Because the organization’s risk from a ransomware incident is \$28,300, it would be justified in spending up to this amount providing ransomware preventive measures such as offline file backups, phishing awareness training, malware detection and prevention, or insurance.

When carrying out a quantitative analysis, some people mistakenly think that the process is purely objective and scientific because data is being presented in numeric values. But a purely quantitative analysis is hard to achieve because there is still some subjectivity when it comes to the data. How do we know that a fire will only take place once every 10 years? How do we know that the damage from a fire will be 25 percent of the value of the asset? We don’t know these values exactly, but instead of just pulling them out of thin air, they should be based upon historical data and industry experience. In quantitative risk analysis, we can do our best to provide all the correct information, and by doing so we will come close to the risk values, but we cannot predict the future and how much future incidents will cost us or the organization.

Results of a Quantitative Risk Analysis

The risk analysis team should have clearly defined goals. The following is a short list of what generally is expected from the results of a risk analysis:

- Monetary values assigned to assets
- Comprehensive list of all significant threats
- Probability of the occurrence rate of each threat
- Loss potential the organization can endure per threat in a 12-month time span
- Recommended controls

Although this list looks short, there is usually an incredible amount of detail under each bullet item. This report will be presented to senior management, which will be concerned with possible monetary losses and the necessary costs to mitigate these risks. Although the report should be as detailed as possible, it should also include an executive summary so that senior management can quickly understand the overall findings of the analysis.

Qualitative Risk Analysis

Another method of risk analysis is *qualitative*, which does not assign numbers and monetary values to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions. (A wide-sweeping analysis can include hundreds of scenarios.) Qualitative analysis techniques include judgment, best practices, intuition, and experience. Examples of qualitative techniques to gather data are Delphi, brainstorming, storyboarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings, and interviews. The risk analysis team will determine the best technique for the threats that need to be assessed, as well as the culture of the organization and individuals involved with the analysis.

The team that is performing the risk analysis gathers personnel who have knowledge of the threats being evaluated. When this group is presented with a scenario that describes threats and loss potential, each member responds with their gut feeling and experience on the likelihood of the threat and the extent of damage that may result. This group explores a scenario of each identified vulnerability and how it would be exploited. The “expert” in the group, who is most familiar with this type of threat, should review the scenario to ensure it reflects how an actual threat would be carried out. Safeguards that would diminish the damage of this threat are then evaluated, and the scenario is played out for each safeguard. The exposure possibility and loss possibility can be ranked as high, medium, or low on a scale of 1 to 5 or 1 to 10.

A common qualitative risk matrix is shown in Figure 2-4. Once the selected personnel rank the likelihood of a threat happening, the loss potential, and the advantages of each

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Figure 2-4 Qualitative risk matrix: likelihood vs. consequences (impact)

The Delphi Technique

The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others' thought processes and enables them to participate in an independent and anonymous way. Each member of the group provides his or her opinion of a certain threat and turns it in to the team that is performing the analysis. The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group. The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

safeguard, this information is compiled into a report and presented to management to help it make better decisions on how best to implement safeguards into the environment. The benefits of this type of analysis are that communication must happen among team members to rank the risks, evaluate the safeguard strengths, and identify weaknesses, and the people who know these subjects the best provide their opinions to management.

Let's look at a *simple* example of a qualitative risk analysis.

The risk analysis team presents a scenario explaining the threat of a hacker accessing confidential information held on the five file servers within the organization. The risk analysis team then distributes the scenario in a written format to a team of five people (the IT manager, database administrator, application programmer, system operator, and operational manager), who are also given a sheet to rank the threat's severity, loss potential, and each safeguard's effectiveness, with a rating of 1 to 5, 1 being the least severe, effective, or probable. Table 2-4 shows the results.

Threat = Hacker Accessing Confidential Information	Severity of Threat	Probability of Threat Taking Place	Potential Loss to the Organization	Effectiveness of Firewall	Effectiveness of Intrusion Detection System	Effectiveness of Honeypot
IT manager	4	2	4	4	3	2
Database administrator	4	4	4	3	4	1
Application programmer	2	3	3	4	2	1
System operator	3	4	3	4	2	1
Operational manager	5	4	4	4	4	2
Results	3.6	3.4	3.6	3.8	3	1.4

Table 2-4 Example of a Qualitative Analysis

This data is compiled and inserted into a report and presented to management. When management is presented with this information, it will see that its staff (or a chosen set) feels that purchasing a firewall will protect the organization from this threat more than purchasing an intrusion detection system (IDS) or setting up a honeypot system.

This is the result of looking at only one threat, and management will view the severity, probability, and loss potential of each threat so it knows which threats cause the greatest risk and should be addressed first.

Quantitative vs. Qualitative

Each method has its advantages and disadvantages, some of which are outlined in Table 2-5 for purposes of comparison.

The risk analysis team, management, risk analysis tools, and culture of the organization will dictate which approach—quantitative or qualitative—should be used. The goal of either method is to estimate an organization's real risk and to rank the severity of the threats so the correct countermeasures can be put into place within a practical budget.

Table 2-5 refers to some of the positive aspects of the quantitative and qualitative approaches. However, not everything is always easy. In deciding to use either a quantitative or qualitative approach, the following points might need to be considered.

Quantitative Cons:

- Calculations can be complex. Can management understand how these values were derived?
- Without automated tools, this process is extremely laborious.
- More preliminary work is needed to gather detailed information about the environment.
- Standards are not available. Each vendor has its own way of interpreting the processes and their results.

Attribute	Quantitative	Qualitative
Requires no calculations		X
Requires more complex calculations	X	
Involves high degree of guesswork		X
Provides general areas and indications of risk		X
Is easier to automate and evaluate	X	
Used in risk management performance tracking	X	
Allows for cost/benefit analysis	X	
Uses independently verifiable and objective metrics	X	
Provides the opinions of the individuals who know the processes best		X
Shows clear-cut losses that can be accrued within one year's time	X	

Table 2-5 Quantitative vs. Qualitative Characteristics

Qualitative Cons:

- The assessments and results are subjective and opinion based.
- Eliminates the opportunity to create a dollar value for cost/benefit discussions.
- Developing a security budget from the results is difficult because monetary values are not used.
- Standards are not available. Each vendor has its own way of interpreting the processes and their results.



NOTE Since a purely quantitative assessment is close to impossible and a purely qualitative process does not provide enough statistical data for financial decisions, these two risk analysis approaches can be used in a hybrid approach. Quantitative evaluation can be used for tangible assets (monetary values), and a qualitative assessment can be used for intangible assets (priority values).

Responding to Risks

Once an organization knows the amount of total and residual risk it is faced with, it must decide how to handle it. Risk can be dealt with in four basic ways: transfer it, avoid it, reduce it, or accept it.

Many types of insurance are available to organizations to protect their assets. If an organization decides the total risk is too high to gamble with, it can purchase insurance, which would *transfer the risk* to the insurance company.

If an organization decides to terminate the activity that is introducing the risk, this is known as *risk avoidance*. For example, if a company allows employees to use instant messaging (IM), there are many risks surrounding this technology. The company could decide not to allow any IM activity by employees because there is not a strong enough business need for its continued use. Discontinuing this service is an example of risk avoidance.

Another approach is *risk mitigation*, where the risk is reduced to a level considered acceptable enough to continue conducting business. The implementation of firewalls, training, and intrusion/detection protection systems or other control types represent types of risk mitigation efforts.

The last approach is to *accept the risk*, which means the organization understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. Many organizations will accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value.

A crucial issue with risk acceptance is understanding why this is the best approach for a specific situation. Unfortunately, today many people in organizations are accepting risk and not understanding fully what they are accepting. This usually has to do with the relative newness of risk management in the security field and the lack of education and experience in those personnel who make risk decisions. When business managers are charged with the responsibility of dealing with risk in their department, most of the time

they will accept whatever risk is put in front of them because their real goals pertain to getting a project finished and out the door. They don't want to be bogged down by this silly and irritating security stuff.

Risk acceptance should be based on several factors. For example, is the potential loss lower than the countermeasure? Can the organization deal with the “pain” that will come with accepting this risk? This second consideration is not purely a cost decision, but may entail noncost issues surrounding the decision. For example, if we accept this risk, we must add three more steps in our production process. Does that make sense for us? Or if we accept this risk, more security incidents may arise from it, and are we prepared to handle those?

The individual or group accepting risk must also understand the potential visibility of this decision. Let's say a company has determined that it is not legally required to protect customers' first names, but that it does have to protect other items like Social Security numbers, account numbers, and so on. So, the company ensures that its current activities are in compliance with the regulations and laws, but what if its customers find out that it is not protecting their full names and they associate this with identity fraud because of their lack of education on the matter? The company may not be able to handle this potential reputation hit, even if it is doing all it is supposed to be doing. Perceptions of a company's customer base are not always rooted in fact, but the possibility that customers will move their business to another company is a potential fact your company must comprehend.

Figure 2-5 shows how a risk management program can be set up, which ties together many of the concepts covered thus far in this chapter.

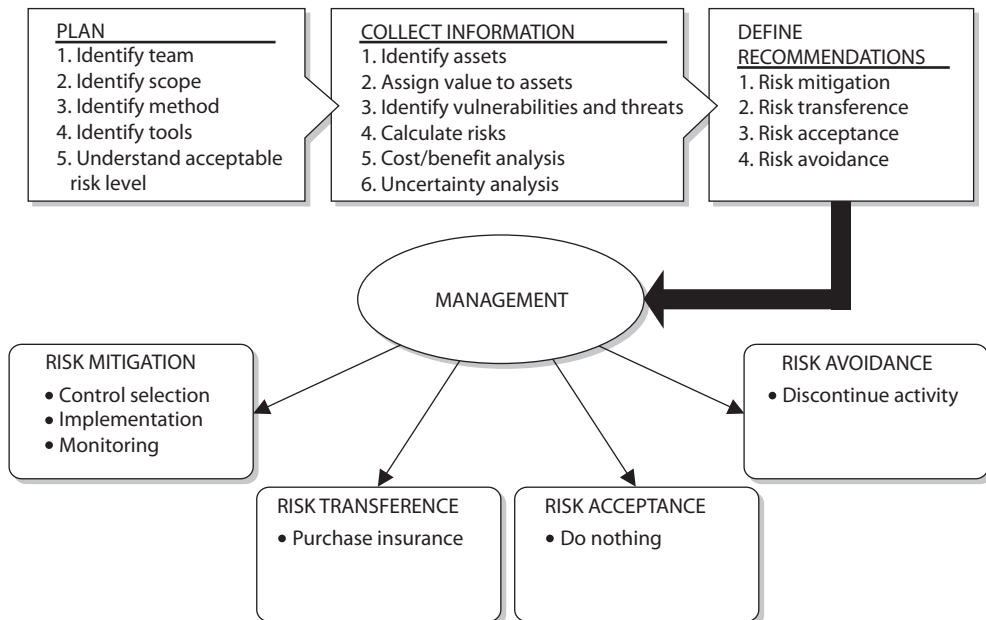


Figure 2-5 How a risk management program can be set up

Total Risk vs. Residual Risk

The reason an organization implements countermeasures is to reduce its overall risk to an acceptable level. As stated earlier, no system or environment is 100 percent secure, which means there is always some risk left over to deal with. This is called *residual risk*.

Residual risk is different from *total risk*, which is the risk an organization faces if it chooses not to implement any type of safeguard. An organization may choose to take on total risk if the cost/benefit analysis results indicate this is the best course of action. For example, if there is a small likelihood that an organization's web servers can be compromised and the necessary safeguards to provide a higher level of protection cost more than the potential loss in the first place, the organization will choose not to implement the safeguard, choosing to deal with the total risk.

There is an important difference between total risk and residual risk and which type of risk an organization is willing to accept. The following are conceptual formulas:

$$\text{threats} \times \text{vulnerability} \times \text{asset value} = \text{total risk}$$
$$(\text{threats} \times \text{vulnerability} \times \text{asset value}) \times \text{controls gap} = \text{residual risk}$$

You may also see these concepts illustrated as the following:

$$\text{total risk} - \text{countermeasures} = \text{residual risk}$$


NOTE The previous formulas are not constructs you can actually plug numbers into. They are instead used to illustrate the relation of the different items that make up risk in a conceptual manner. This means no multiplication or mathematical functions actually take place. It is a means of understanding what items are involved when defining either total or residual risk.

During a risk assessment, the threats and vulnerabilities are identified. The possibility of a vulnerability being exploited is multiplied by the value of the assets being assessed, which results in the total risk. Once the controls gap (protection the control cannot provide) is factored in, the result is the residual risk. Implementing countermeasures is a way of mitigating risks. Because no organization can remove all threats, there will always be some residual risk. The question is what level of risk the organization is willing to accept.

Countermeasure Selection and Implementation

Countermeasures are the means by which we reduce specific risks to acceptable levels. This section addresses identifying and choosing the right countermeasures for computer systems. It gives the best attributes to look for and the different cost scenarios to investigate when comparing different types of countermeasures. The end product of the analysis of choices should demonstrate why the selected control is the most advantageous to the organization.



NOTE The terms control, countermeasure, safeguard, security mechanism, and protection mechanism are synonymous in the context of information systems security. We use them interchangeably.

Control Selection

A security control must make good business sense, meaning it is cost-effective (its benefit outweighs its cost). This requires another type of analysis: a *cost/benefit analysis*. A commonly used cost/benefit calculation for a given safeguard (control) is

$$(\text{ALE before implementing safeguard}) - (\text{ALE after implementing safeguard}) - (\text{annual cost of safeguard}) = \text{value of safeguard to the organization}$$

For example, if the ALE of the threat of a hacker bringing down a web server is \$12,000 prior to implementing the suggested safeguard, and the ALE is \$3,000 after implementing the safeguard, while the annual cost of maintenance and operation of the safeguard is \$650, then the value of this safeguard to the organization is \$8,350 each year.

Recall that the ALE has two factors, the single loss expectancy and the annual rate of occurrence, so safeguards can decrease either or both. The countermeasure referenced in the previous example could aim to reduce the costs associated with restoring the web server, or make it less likely that it is brought down, or both. All too often, we focus our attention on making the threat less likely, while, in some cases, it might be less expensive to make it easier to recover.

The cost of a countermeasure is more than just the amount filled out on the purchase order. The following items should be considered and evaluated when deriving the full cost of a countermeasure:

- Product costs
- Design/planning costs
- Implementation costs
- Environment modifications (both physical and logical)
- Compatibility with other countermeasures
- Maintenance requirements
- Testing requirements
- Repair, replacement, or update costs
- Operating and support costs
- Effects on productivity
- Subscription costs
- Extra staff-hours for monitoring and responding to alerts

Many organizations have gone through the pain of purchasing new security products without understanding that they will need the staff to maintain those products. Although tools automate tasks, many organizations were not even carrying out these tasks before, so they do not save on staff-hours, but many times require more hours. For example, Company A decides that to protect many of its resources, purchasing an intrusion detection system is warranted. So, the company pays \$5,500 for an IDS. Is that the total cost? Nope. This software should be tested in an environment that is segmented from the production environment to uncover any unexpected activity. After this testing is complete and the security group feels it is safe to insert the IDS into its production environment, the security group must install the monitoring management software, install the sensors, and properly direct the communication paths from the sensors to the management console. The security group may also need to reconfigure the routers to redirect traffic flow, and it definitely needs to ensure that users cannot access the IDS management console. Finally, the security group should configure a database to hold all attack signatures and then run simulations.

Costs associated with an IDS alert response should most definitely be considered. Now that Company A has an IDS in place, security administrators may need additional alerting equipment such as smartphones. And then there are the time costs associated with a response to an IDS event.

Anyone who has worked in an IT group knows that some adverse reaction almost always takes place in this type of scenario. Network performance can take an unacceptable hit after installing a product if it is an inline or proactive product. Users may no longer be able to access a server for some mysterious reason. The IDS vendor may not have explained that two more service patches are necessary for the whole thing to work correctly. Staff time will need to be allocated for training and to respond to all of the alerts (true or false) the new IDS sends out.

So, for example, the cost of this countermeasure could be \$23,500 for the product and licenses; \$2,500 for training; \$3,400 for testing; \$2,600 for the loss in user productivity once the product is introduced into production; and \$4,000 in labor for router reconfiguration, product installation, troubleshooting, and installation of the two service patches. The real cost of this countermeasure is \$36,000. If our total potential loss was calculated at \$9,000, we went over budget by 300 percent when applying this countermeasure for the identified risk. Some of these costs may be hard or impossible to identify before they are incurred, but an experienced risk analyst would account for many of these possibilities.

Types of Controls

In our examples so far, we've focused on countermeasures like firewalls and IDSs, but there are many more options. Controls come in three main categories: administrative, technical, and physical. *Administrative controls* are commonly referred to as "soft controls" because they are more management oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. *Technical controls* (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, and identification and authentication mechanisms. And *physical controls*

are items put into place to protect facilities, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

These control categories need to be put into place to provide *defense-in-depth*, which is the coordinated use of multiple security controls in a layered approach, as shown in Figure 2-6. A multilayered defense system minimizes the probability of successful penetration and compromise because an attacker would have to get through several different types of protection mechanisms before she gained access to the critical assets. For example, Company A can have the following physical controls in place that work in a layered model:

- Fence
- Locked external doors
- Closed-circuit TV (CCTV)
- Security guard
- Locked internal doors
- Locked server room
- Physically secured computers (cable locks)

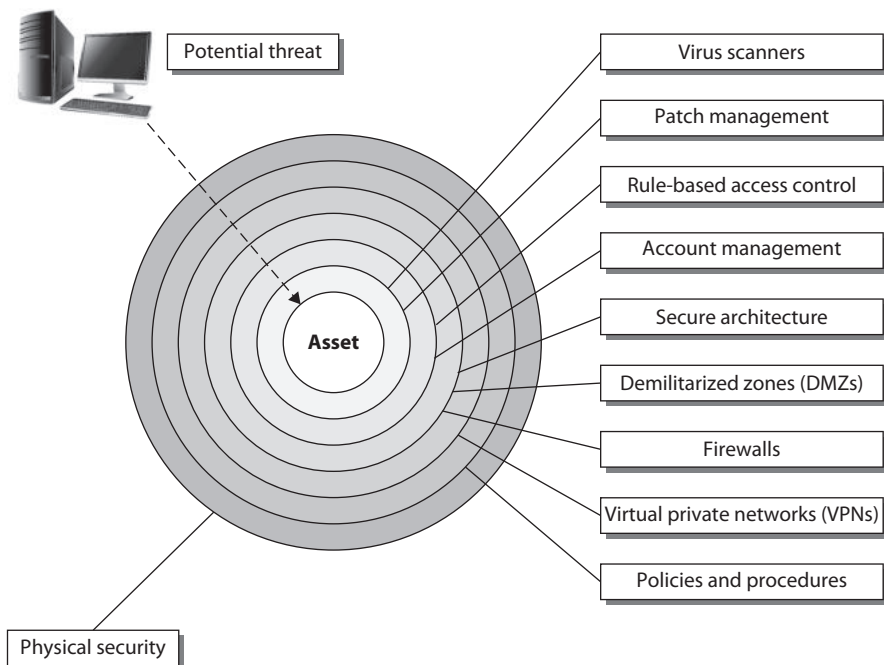


Figure 2-6 Defense-in-depth

Technical controls that are commonly put into place to provide this type of layered approach are

- Firewalls
- Intrusion detection system
- Intrusion prevention system
- Antimalware
- Access control
- Encryption

The types of controls that are actually implemented must map to the threats the organization faces, and the number of layers that are put into place must map to the sensitivity of the asset. The rule of thumb is the more sensitive the asset, the more layers of protection that must be put into place.

So the different *categories* of controls that can be used are administrative, technical, and physical. But what do these controls actually *do* for us? We need to understand what the different control types can provide us in our quest to secure our environments.

The different types of security controls are *preventive*, *detective*, *corrective*, *deterrent*, *recovery*, and *compensating*. By having a better understanding of the different control types, you will be able to make more informed decisions about what controls will be best used in specific situations. The six different control types are as follows:

- **Preventive** Intended to avoid an incident from occurring
- **Detective** Helps identify an incident's activities and potentially an intruder
- **Corrective** Fixes components or systems after an incident has occurred
- **Deterrent** Intended to discourage a potential attacker
- **Recovery** Intended to bring the environment back to regular operations
- **Compensating** Provides an alternative measure of control

Once you understand fully what the different controls do, you can use them in the right locations for specific risks.

When looking at a security structure of an environment, it is most productive to use a preventive model and then use detective, corrective, and recovery mechanisms to help support this model. Basically, you want to stop any trouble before it starts, but you must be able to quickly react and combat trouble if it does find you. It is not feasible to prevent everything; therefore, what you cannot prevent, you should be able to quickly detect. That's why preventive and detective controls should always be implemented together and should complement each other. To take this concept further: what you can't prevent, you should be able to detect, and if you detect something, it means you weren't able to prevent it, and therefore you should take corrective action to make sure it is indeed prevented the next time around. Therefore, all three types work together: preventive, detective, and corrective.

The control types described next (administrative, physical, and technical) are preventive in nature. These are important to understand when developing an enterprise-wide security program. Obviously, these are only provided as illustrative examples. Keep in mind as you go over them that a specific control may fall within multiple classifications. For example, most security cameras could be considered preventive (since they may dissuade criminals from breaking in if they are highly visible), detective (if there is a person monitoring them live), and corrective (if they are used to track a criminal that breached your physical perimeter).

Preventive: Administrative

- Policies and procedures
- Effective hiring practices
- Pre-employment background checks
- Controlled termination processes
- Data classification and labeling
- Security awareness

Preventive: Physical

- Badges, swipe cards
- Guards, dogs
- Fences, locks, mantraps

Preventive: Technical

- Passwords, biometrics, smart cards
- Encryption, secure protocols, call-back systems, database views, constrained user interfaces
- Antimalware software, access control lists, firewalls, IPS

Table 2-6 shows how these types of control mechanisms perform different security functions. Many students get themselves wrapped around the axle when trying to get their mind around which control provides which functionality. This is how this train of thought usually takes place: “A security camera system is a detective control, but if an attacker sees its cameras, it could be a deterrent.” Let’s stop right here. Do not make this any harder than it has to be. When trying to map the functionality requirement to a control, think of the *main* reason that control would be put into place. A firewall tries to prevent something bad from taking place, so it is a preventive control. Auditing logs is done after an event took place, so it is detective. A data backup system is developed so that data can be recovered; thus, this is a recovery control. Computer images are created so that if software gets corrupted, they can be reloaded; thus, this is a corrective control.

Note that some controls can serve different functions. Security guards can deter would-be attackers, but if they don’t deter all of them, they can also stop (prevent)

Control Type:	Preventive	Detective	Corrective	Deterrent	Recovery	Compensating
Controls by Category:						
Physical						
Fences				X		
Locks	X					
Badge system	X					
Security guard	X	X	X	X		
Mantrap doors	X					
Lighting				X		
Motion detectors		X				
Closed-circuit TVs		X				
Offsite facility					X	X
Administrative						
Security policy	X					X
Monitoring and supervising		X				X
Separation of duties	X					
Job rotation		X		X		
Information classification	X					
Investigations		X				
Security awareness training	X					
Technical						
ACLs	X					
Encryption	X					
Audit logs		X				
IDS		X				
Antimalware software	X	X				
Workstation images			X			
Smart cards	X					
Data backup					X	

Table 2-6 Control Categories and Types

the ones that try to get into a facility. Perhaps the attacker was particularly sneaky and he managed to get into an office building, in which case the security guards can be detective controls as they make the rounds and even corrective controls when they find the intruder, call law enforcement, and escort the attacker out of the building and into the backseat of a police car. When taking the CISSP exam, look for clues in the question to determine which functionality is most relevant.

One control functionality that some people struggle with is a compensating control. Let's look at some examples of compensating controls to best explain their function. If your organization needed to implement strong physical security, you might suggest to management that they employ security guards. But after calculating all the costs of security guards, your organization might decide to use a compensating (alternative) control that provides similar protection but is more affordable—as in a fence. In another example, let's say you are a security administrator and you are in charge of maintaining the organization's firewalls. Management tells you that a certain protocol that you know is vulnerable to exploitation has to be allowed through the firewall for business reasons. The network needs to be protected by a compensating (alternative) control pertaining to this protocol, which may be setting up a proxy server for that specific traffic type to ensure that it is properly inspected and controlled. So a compensating control is just an alternative control that provides similar protection as the original control but has to be used because it is more affordable or allows specifically required business functionality.

Several types of security controls exist, and they all need to work together. The complexity of the controls and of the environment they are in can cause the controls to contradict each other or leave gaps in security. This can introduce unforeseen holes in the organization's protection that are not fully understood by the implementers. An organization may have very strict technical access controls in place and all the necessary administrative controls up to snuff, but if any person is allowed to physically access any system in the facility, then clear security dangers are present within the environment. Together, these controls should work in harmony to provide a healthy, safe, and productive environment.

The risk assessment team must evaluate the security controls' functionality and effectiveness. When selecting a security control, some attributes are more favorable than others. Table 2-7 lists and describes attributes that should be considered before purchasing and committing to a security control.

Security controls can provide deterrence attributes if they are highly visible. This tells potential evildoers that adequate protection is in place and that they should move on to an easier target. Although the control may be highly visible, attackers should not be able to discover the way it works, thus enabling them to attempt to modify it, or know how to get around the protection mechanism. If users know how to disable the antimalware program that is taking up CPU cycles or know how to bypass a proxy server to get to the Internet without restrictions, they will do so.

Control Assessments

Once you select the administrative, technical, and physical controls that you think will reduce your risks to acceptable levels, you have to ensure that this is actually the case.

Characteristic	Description
Modular	The control can be installed or removed from an environment without adversely affecting other mechanisms.
Provides uniform protection	A security level is applied in a standardized method to all mechanisms the control is designed to protect.
Provides override functionality	An administrator can override the restriction if necessary.
Defaults to least privilege	When installed, the control defaults to a lack of permissions and rights instead of installing with everyone having full control.
Independence of control and the asset it is protecting	The given control can protect multiple assets, and a given asset can be protected by multiple controls.
Flexibility and security	The more security the control provides, the better. This functionality should come with flexibility, which enables you to choose different functions instead of all or none.
Usability	The control does not needlessly interfere with users' work.
Asset protection	The asset is still protected even if the countermeasure needs to be reset.
Easily upgraded	Software continues to evolve, and updates should be able to happen painlessly.
Auditing functionality	The control includes a mechanism that provides auditing at various levels of verbosity.
Minimizes dependence on other components	The control should be flexible and not have strict requirements about the environment into which it will be installed.
Must produce output in usable and understandable format	The control should present important information in a format easy for humans to understand and use for trend analysis.
Testable	The control should be able to be tested in different environments under different situations.
Does not introduce other compromises	The control should not provide any covert channels or back doors.
System and user performance	System and user performance should not be greatly affected by the control.
Proper alerting	The control should have the capability for thresholds to be set as to when to alert personnel of a security breach, and this type of alert should be acceptable.
Does not affect assets	The assets in the environment should not be adversely affected by the control.

Table 2-7 Characteristics to Consider When Assessing Security Controls

A *control assessment* is an evaluation of one or more controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome. Let's look at each of those test elements in turn using anonymized examples from the real world.

You may have chosen the right control for a given risk, but you also need *verification* that the manner in which it is implemented is correct too. Let's suppose you decide to upgrade a firewall to mitigate a number of risks you've identified. You invest a ton of money in the latest and greatest firewall and apply a bunch of rules to filter out the good from the bad. And yet, you forget to change the administrator's default password, and an attacker is able to log into your firewall, lock out the security team by changing the password, and then change the rules to allow malicious traffic through. The technical control was good, it just wasn't implemented correctly. You avoid this by developing a thorough set of tests that look at every aspect of the implementation and ensure no steps were skipped or done wrong.

Another aspect of verification is to ensure that the controls are operating as intended. You may have implemented the control correctly, but there are many reasons why it may not work as you expected it would. For example, suppose you implement a policy that all personnel in a facility must wear identification badges. Employees, contractors, and visitors each get their own unique badge design to differentiate them. The policy is implemented, and all staff are trained on it, but after a few weeks people get complacent and stop noticing whether they (or others) are wearing badges. The administrative control was properly implemented but is not working as intended. The control assessment should include operational checks, such as having different people (perhaps some who are well known in the organization and some who are not part of it) walk through the facility with no badges and see whether they are challenged or reported.

Finally, we want *validation* that the controls are producing the desired outcomes. Controls are selected for the purpose of reducing risk...so are they? Suppose you install temperature sensors in your data center that generate alarms whenever they get too hot. You are trying to reduce the risk of hardware failures due to high temperatures. These physical controls are properly installed and work as intended. In fact, they generate alarms every day during peak usage hours. Are they reducing the risk? Unless you upgrade the underpowered air conditioning unit, all these alarms will do nothing to help you avoid outages. Any assessment of your controls must explicitly test whether the risk for which they were selected is actually being reduced.



EXAM TIP An easy way to differentiate verification and validation is that verification answers the question "did we implement the control right?" while validation answers the question "did we implement the right control?"

Security and Privacy

Security effectiveness deals with metrics such as meeting service level agreement (SLA) requirements, achieving returns on investment (ROIs), meeting set baselines, and providing management with a dashboard or balanced scorecard system. These are ways to determine how useful the current security solutions and architecture as a whole are performing.

Another side to assessing security controls is ensuring that they do not violate our privacy policies and regulations. It does us no good to implement the best security controls if they require gross violations of people's right to keep certain information

about themselves from being known or used in inappropriate ways. For example, an organization could have a policy that allows employees to use the organization's assets for personal purposes while they are on breaks. The same organization has implemented Transport Layer Security (TLS) proxies that decrypt all network traffic in order to conduct deep packet analysis and mitigate the risk that a threat actor is using encryption to hide her malicious deeds. Normally, the process is fully automated and no other staff members look at the decrypted communications. Periodically, however, security staff manually check the system to ensure everything is working properly. Now, suppose an employee reveals some very private health information to a friend over her personal webmail and that traffic is monitored and observed by a security staffer. That breach of privacy could cause a multitude of ethical, regulatory, and even legal problems for the organization.

When implementing security controls, it is critical to consider their privacy implications. If your organization has a chief privacy officer (or other privacy professional), that person should be part of the process of selecting and implementing security controls to ensure they don't unduly (or even illegally) violate employee privacy.

Monitoring Risks

We really can't just build a risk management program (or any program, for that matter), call it good, and go home. We need a way to assess the effectiveness of our work, identify deficiencies, and prioritize the things that still need work. We need a way to facilitate decision making, performance improvement, and accountability through collection, analysis, and reporting of the necessary information. More importantly, we need to be able to identify changes in the environment and be able to understand their impacts on our risk posture. All this needs to be based on facts and metrics. As the saying goes, "You can't manage something you can't measure."

Risk monitoring is the ongoing process of adding new risks, reevaluating existing ones, removing moot ones, and continuously assessing the effectiveness of our controls at mitigating all risks to tolerable levels. Risk monitoring activities should be focused on three key areas: effectiveness, change, and compliance. The risk management team should continually look for improvement opportunities, periodically analyze the data gathered from each key area, and report its findings to senior management. Let's take a closer look at how we might go about monitoring and measuring each area.

Effectiveness Monitoring

There are many reasons why the effectiveness of our security controls decreases. Technical controls may not adapt quickly to changing threat actor behaviors. Employees may lose awareness of (or interest in) administrative controls. Physical controls may not keep up with changing behaviors as people move in and through our facilities. How do we measure this decline in the effectiveness of our controls and, more importantly, the rising risks to our organizations? This is the crux of effectiveness monitoring.

One approach is to keep track of the number of security incidents by severity. Let's say that we implemented controls to reduce the risk of ransomware attacks. We redesigned our security awareness training, deployed a new endpoint detection and

response (EDR) solution, and implemented an automated offline backup system. Subsequently, the number of ransomware-related incidents sharply declined across all severity categories. While we still see a handful of localized cases here and there, no data is lost, nobody is forced offline, and business is humming. However, recently we are noticing that the number of low-severity incidents has started to increase. These are cases where the ransomware makes it onto a workstation but is stopped as it attempts to encrypt files. If we're not paying attention to this trend, we may miss the fact that the malware is evolving and becoming more effective at evading our EDR solution. We'd be giving the adversary a huge advantage by letting them experiment and improve while we do nothing about it. This is why effectiveness monitoring is important, and why it has to be tied to specific metrics that can be quantified and analyzed over time.

In the previous example, the metric was the number of incidents related to ransomware in our environment. There are many other metrics you could use, depending on the control in question. You could use a red team and measure the number of times it is successful at compromising various assets. You could use the number of suspected phishing attacks reported by alert employees. Whatever your approach, you should determine the effectiveness metrics you'll use to monitor controls when you decide to use those controls. Then, you really need to track those metrics over time to identify trends. Failure to do so will result, almost inevitably, in the gradual (or perhaps sudden) increase in risk until, one sad day, it is realized.



NOTE The Center for Internet Security (CIS) publishes a helpful (and free) document titled "CIS Controls Measures and Metrics," currently in its seventh version. It provides specific measures for each control as well as goals for their values in your organization.

A good way to enable effectiveness monitoring is to establish a standing group that periodically checks known threats and the controls that are meant to mitigate them. An example of this is a threat working group (TWG), which consists of members of all major parts of the organization, meeting regularly (say, monthly) to review the list of risks (sometimes called a risk registry) and ensure that threats and controls remain valid. The TWG assigns owners to each risk and ensures those persons or groups are keeping up their responsibilities. The TWG can also be the focal point for scheduling security assessments, be they internal or external, to verify and validate the controls.

Change Monitoring

Even if you keep track of known threats and the risks they pose, it is likely that changes in your organization's environment will introduce new risks. There are two major sources of change that impact your overall risk: information systems and business. The first is perhaps the most obvious to cybersecurity professionals. A new system is introduced, an old one retired, or an existing one updated or reconfigured. Any of these changes can produce new risks or change those you are already tracking. Another source of changes that introduce risks is the business itself. Over time, your organization will embark on new ventures, change internal processes, or perhaps merge with or acquire another organization.

All these changes need to be carefully analyzed to ensure an accurate understanding of their effects on the overall risk posture.

Monitoring changes to your environment and dealing with the risks they could introduce is part of a good change management process. Typically, organizations will have a change advisory board (CAB) or a similarly named standing group that reviews and approves any changes such as the development of new policies, systems, and business processes. The CAB measures changes through a variety of metrics that also are used to monitor risks, such as the following:

- Number of unauthorized changes
- Average time to implement a change
- Number of failed changes
- Number of security incidents attributable to changes



NOTE We will discuss change management in more detail in Chapter 19.

Compliance Monitoring

Something else that could change in your organization and affect your risk are legal, regulatory, and policy requirements. Compliance monitoring is a bit easier than effectiveness monitoring and change monitoring, because compliance tends to change fairly infrequently. Laws and external regulations usually take years to change, while internal regulations and policies should be part of the change management process we discussed previously. Though the frequency of compliance changes is fairly low, these changes can have significant impacts in the organization. A great example of this is the General Data Protection Regulation (GDPR) that came into effect in May 2018. It was years in the making, but it has had huge effects on any organization that stores or processes data belonging to a person from the European Union (EU).

Another aspect of compliance monitoring is responding to audit findings. Whether it is an external or internal audit, any findings dealing with compliance need to be addressed. If the audit reveals risks that are improperly mitigated, the risk team needs to respond to them. Failure to do so could result in significant fines or even criminal charges.

So, what can we measure to monitor our compliance? It varies among organizations, but here are some common metrics to consider:

- Number of audit findings
- Ratio of internal (i.e., self-discovered) to external (i.e., audit) inquiries
- Average time to close an inquiry
- Number of internal disciplinary actions related to compliance

No organization is perfectly compliant all the time, so there is always an element of compliance risk. These risks, however, increase dramatically if there is no formal process for searching for and dealing with issues that violate policies, regulations, or laws.

Risk Reporting

Risk reporting is an essential component of risk management in general and risk monitoring in particular. (Recall that risk management encompasses framing, assessing, responding to, and monitoring the risks.) Reporting enables organizational decision-making, security governance, and day-to-day operations. It is also important for compliance purposes.

So, how *should* we report risks? There is no set formula for reporting, but there are a couple of guiding principles. The first one is to understand the audience. There are at least three groups at which you may target risk reports: executives (and board members), managers, and risk owners. Each requires a different approach.

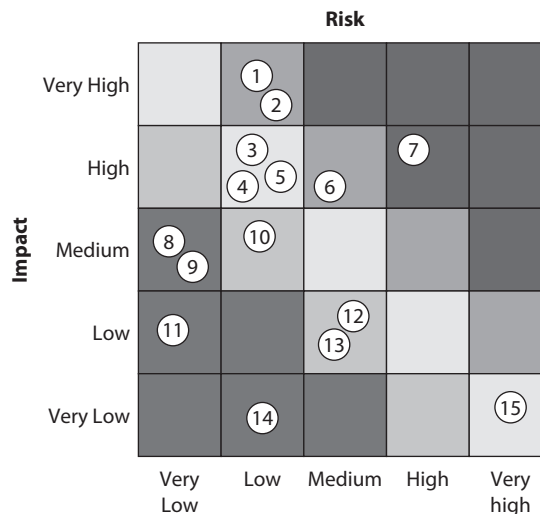
Executives and Board Members

Senior leaders in an organization are generally not interested in the details, nor should they be. Their role is to set and monitor the strategic direction, not to run day-to-day operations. These leaders want to know whether risks can be properly mitigated or require change to the organizational strategy. They will be interested in the biggest risks to the organization and will want to know what is being done to address them. Executives and board members should also be briefed on risks that have been “accepted” and what their potential impacts could be.

When dealing with senior decision makers, risk heat maps, such as illustrated in Figure 2-7, are typically used rather than verbose descriptions. This is to ensure that these leaders can get the information they need at a glance in order to decide whether strategic adjustments may be needed. In Figure 2-7, board members likely would be interested in

Figure 2-7

Sample risk heat map



discussing risk item #7 first since it is particularly significant. That is the point of a heat map: it allows senior-level audiences to home in on the important topics for discussion.

Managers

Managers across the organization will need much more detailed reports because they are responsible for, well, managing the risks. They will want to know current risks and how they've been trending over time. Are risks decreasing or increasing? Either way, why? Where does progress seem to be stuck? These are some of the questions managers will want the report to answer. They will also want to be able to drill into specific items of interest to get into the details, such as who owns the risk, how we are responding to the risk, and why the current approach may not be working.

Many organizations rely on risk management dashboards for this level of reporting. These dashboards may be part of a risk management tool, in which case they'd be interactive and allow drilling into specific items in the report. Organizations without these automated tools typically use spreadsheets to generate graphs (showing trends over time) or even manually developed slides. Whatever the approach, the idea is to present actionable information allowing business unit managers to track their progress over time with respect to risks.

Risk Owners

This is the internal audience that needs the most detailed reporting, because the risk owners are the staff members responsible for managing individual risks. They take direction from management as they respond to specific risks. For example, if the organization decides to transfer a given risk, the risk owner will be responsible for ensuring the insurance policy is developed and acquired effectively. This will include performance indicators, such as cost, coverage, and responsiveness. Cybersecurity insurance companies often require that certain controls be in place in order to provide coverage, so the risk owner must also ensure that these conditions are met so that the premiums are not being paid in vain.

Continuous Improvement

Only by reassessing the risks on a periodic basis can the risk management team's statements on security control performance be trusted. If the risk has not changed and the safeguards implemented are functioning in good order, then it can be said that the risk is being properly mitigated. Regular risk management monitoring will support the information security risk ratings.

Vulnerability analysis and continued asset identification and valuation are also important tasks of risk management monitoring and performance. The cycle of continued risk analysis is a very important part of determining whether the safeguard controls that have been put in place are appropriate and necessary to safeguard the assets and environment.

Continuous improvement is the practice of identifying opportunities, mitigating threats, improving quality, and reducing waste as an ongoing effort. It is the hallmark of mature and effective organizations.

Level	Maturity	Characteristics
1	Initial	Risk activities are ad hoc, reactive, and poorly controlled.
2	Repeatable	Procedures are documented and (mostly) followed.
3	Defined	Standard procedures, tools, and methods are applied consistently.
4	Managed	Quantitative methods are applied both to risk management and to the program.
5	Optimizing	Data-driven innovation occurs across the entire organization.

Table 2-8 Typical Maturity Model

Risk Maturity Modeling

Maturity models are tools that allow us to determine the ability of our organizations for continuous improvement. We generally assess the maturity of an organization's risk management on a scale of 1 to 5, as shown in Table 2-8. There is actually a level 0, which is where the organization is not managing risk at all.

While it may be tempting to think that we should all strive to achieve the highest level of maturity with regard to risk management, the reality is that we should reach the right level of maturity given our resources, strategies, and business environment. It would make little sense for a very small retail company to strive for level 5, because doing so would require a level of resource investment that is not realistic. Conversely, it would be a very bad idea for a large enterprise in the defense industry to be satisfied with a maturity level 1, because the risks it faces are substantial. Ultimately, the level of maturity that makes sense is a business decision, not a cybersecurity one.

Supply Chain Risk Management

Many organizations fail to consider their supply chain when managing risk, despite the fact that it often presents a convenient and easier back door to an attacker. So what is a supply chain anyway? A supply chain is a sequence of suppliers involved in delivering some product. If your company manufactures laptops, your supply chain will include the vendor that supplies your video cards. It will also include whoever makes the integrated circuits that go on those cards, as well as the supplier of the raw chemicals that are involved in that process. The supply chain also includes suppliers of services, such as the company that maintains the heating, ventilation, and air conditioning (HVAC) systems needed to keep your assembly lines running.

The various organizations that make up your supply chain will have a different outlook on security than you do. For one thing, their threat modeling will include different threats than yours. Why would a criminal looking to steal credit card information target an HVAC service provider? This is exactly what happened in 2013 when Target had over 40 million credit cards compromised. Target had done a reasonable job at securing its perimeter, but not its internal networks. The attacker, unable (or maybe just unwilling) to penetrate Target's outer shell head-on, decided to exploit the vulnerable network of one of Target's HVAC service providers and steal its credentials. Armed with these, the

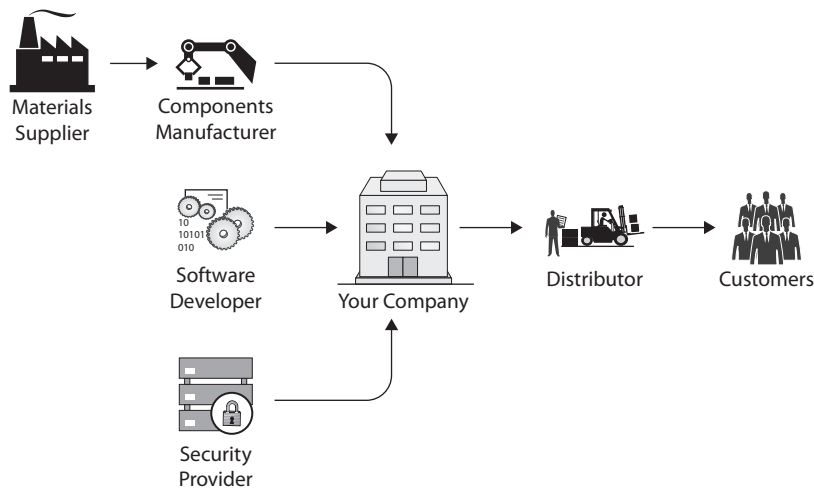
thieves were able to gain access to the point of sale terminals and, from there, the credit card information.

The basic processes you'll need to implement to manage risk in your supply chain are the same ones you use in the rest of your risk management program. The differences are mainly in what you look at (that is, the scope of your assessments) and what you can do about it (legally and contractually). A good resource to help integrate supply chain risk into your risk management program is NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

One of the first things you'll need to do is to create a supply chain map for your organization. This is essentially a network diagram of who supplies what to whom, down to your ultimate customers. Figure 2-8 depicts a simplified systems integrator company ("Your Company"). It has a hardware components manufacturer that supplies it hardware and is, in turn, supplied by a materials producer. Your Company receives software from a developer and receives managed security from an external service provider. The hardware and software components are integrated and configured into Your Company's product, which is then shipped to its distributor and on to its customers. In this example, the company has four suppliers on which to base its supply chain risk assessment. It is also considered a supplier to its distributor.

Now, suppose the software developer in Figure 2-8 is attacked and the threat actors insert malicious code into the developer's software product. Anyone who receives that application from Your Company, or perhaps through an otherwise legitimate software update, also gets a very stealthy piece of malware that "phones home" to these actors, telling them where the malware is and what its host network looks like. These are sophisticated, nation-state spies intent on remaining undetected while they penetrate some very specific targets. If an infected organization is of interest to them, they'll deliver the next stage of malware with which to quietly explore and steal files. Otherwise, they'll

Figure 2-8
Simplified supply chain



tell the malware to go dormant, making their actions extremely difficult to detect. This is a high-level description of a cyber campaign discovered in late 2020 that exploited the Orion software developed by U.S.-based firm SolarWinds. The magnitude of this series of attacks underscores the importance of managing risk introduced by your suppliers.

Upstream and Downstream Suppliers

Suppliers are “upstream” from your company if they supply materials, goods, or services to your company and your company uses those in turn to provide whatever it is that it supplies to others. The core vulnerability that exists in these supply arrangements is that you could allow untrusted hardware, software, or services into your organization or products, where they could cause security problems. The Greeks used this to their advantage against the Trojans.

Conversely, your company may be upstream from others in the same supply chain. These would be your company’s downstream suppliers. While it may be tempting to think that you should be concerned only about supply chain security upstream, those who follow your company in the supply chain may have their own set of upstream requirements for your firm. Furthermore, your customers may not care that a security issue was caused by your downstream distributor; your brand name could be damaged all the same.

Risks Associated with Hardware, Software, and Services

While we explore risks inherent in *any* hardware, software, and services later in this book, for now let’s consider those risks that are specifically tied to supply chains. That is to say, what risks do you face when you acquire something (or someone’s service) and insert it into your information systems?

Hardware

One of the major supply chain risks is the addition of hardware Trojans to electronic components. A hardware Trojan is an electronic circuit that is added to an existing device in order to compromise its security or provide unauthorized functionality. Depending on the attacker’s access, these mechanisms can be inserted at any stage of the hardware development process (specification, design, fabrication, testing, assembly, or packaging). It is also possible to add them after the hardware is packaged by intercepting shipments in the supply chain. In this case, the Trojan may be noticeable if the device is opened and visually inspected. The earlier in the supply chain that hardware Trojans are inserted, the more difficult they are to detect.

Another supply chain risk to hardware is the substitution of counterfeit components. The problems with these clones are many, but from a security perspective one of the most important is that they don’t go through the same quality controls that the real ones do. This leads to lower reliability and abnormal behavior. It could also lead to undetected hardware Trojans (perhaps inserted by the illicit manufacturers themselves). Obviously, using counterfeits could have legal implications and will definitely be a problem when you need customer support from the manufacturer.

Software

Like hardware, third-party software can be Trojaned by an adversary in your supply chain, particularly if it is custom-made for your organization. This could happen if your supplier reuses components (like libraries) developed elsewhere and to which the attacker has access. It can also be done by a malicious insider working for the supplier or by a remote attacker who has gained access to the supplier's software repositories. Failing all that, the software could be intercepted in transit to you, modified, and then sent on its way. This last approach could be made more difficult for the adversary by using code signing or hashes, but it is still possible.

Services

More organizations are outsourcing services to allow them to focus on their core business functions. Organizations use hosting companies to maintain websites and e-mail servers, service providers for various telecommunication connections, disaster recovery companies for co-location capabilities, cloud computing providers for infrastructure or application services, developers for software creation, and security companies to carry out vulnerability management. It is important to realize that while you can outsource functionality, you cannot outsource risk. When your organization is using these third-party service providers, it can still be ultimately responsible if something like a data breach takes place. The following are some things an organization should do to reduce its risk when outsourcing:

- Review the service provider's security program
- Conduct onsite inspection and interviews
- Review contracts to ensure security and protection levels are agreed upon
- Ensure service level agreements are in place
- Review internal and external audit reports and third-party reviews
- Review references and communicate with former and existing customers
- Review Better Business Bureau reports
- Ensure the service provider has a business continuity plan (BCP) in place
- Implement a nondisclosure agreement (NDA)
- Understand the provider's legal and regulatory requirements

Service outsourcing is prevalent within organizations today but is commonly forgotten about when it comes to security and compliance requirements. It may be economical to outsource certain functionalities, but if this allows security breaches to take place, it can turn out to be a very costly decision.

Other Third-Party Risks

An organization's supply chain is not its only source of third-party risks. There are many other ways in which organizations may be dependent on each other that don't really fit the

supplier–consumer model. For example, many companies have a network of channel partners that help them directly or indirectly sell products. Others engage in general or limited partnerships for specific projects, and these relationships require sharing some resources and risks. Most organizations nowadays have a complex web of (sometimes not so obvious) third parties on whom they rely to some extent and who, therefore, introduce risks.

Minimum Security Requirements

The key to effectively mitigating risks to an organization introduced by its suppliers is to clearly state each party's requirements in the contract or agreement that governs their relationship. In terms of cybersecurity, this includes whatever measures are needed to protect sensitive data at rest, in transit, and in use. It also includes the actions the supplier shall perform should the data become compromised, as well as the means through which the purchasing organization may proactively verify compliance. In summary, the critical classes of requirements that should be included in a contractual agreement are as follows.

- **Data protection** Proactive cybersecurity measures
- **Incident response** Reactive cybersecurity measures
- **Verification means** Ways in which the customer may verify the preceding requirements

If any requirements are missing, ambiguously stated, or otherwise vitiated, the supplier agreement can become void, voidable, or unenforceable. So, how do you verify that your supplier is complying with all contractual requirements dealing with risk? Third-party assessments are considered best practice and may be required for compliance (e.g., with PCI DSS). The following are some examples of external evaluations that would indicate a supplier's ability to comply with its contractual obligations:

- ISO 27001 certification
- U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC)
- Payment Card Industry Digital Security Standard (PCI DSS) certification
- Service Organization Control 1 (SOC1) or 2 (SOC2) report
- U.S. Federal Risk and Authorization Management Program (FedRAMP) authorization



NOTE We will discuss these third-party evaluations in subsequent chapters.

Other third-party evaluations, such as vulnerability assessments and penetration tests, are helpful in establishing a baseline of security in the organization. However, by themselves, these limited-scope tests are insufficient to verify that the supplier is able to fulfill its contractual obligations.

Service Level Agreements

A *service level agreement (SLA)* is a contractual agreement that states that a service provider guarantees a certain level of service. If the service is not delivered at the agreed-upon level (or better), then there are consequences (typically financial) for the service provider. SLAs provide a mechanism to mitigate some of the risk from service providers in the supply chain. For example, an Internet service provider (ISP) may sign an SLA of 99.999 percent (commonly called “five nines”) uptime to the Internet backbone. That means that the ISP guarantees less than 26 seconds of downtime per month.

Business Continuity

Though we strive to drive down the risks of negative effects in our organizations, we can be sure that sooner or later an event will slip through and cause negative impacts. Ideally, the losses are contained and won't affect the major business efforts. However, as security professionals we need to have plans in place for when the unthinkable happens. Under those extreme (and sometimes unpredictable) conditions, we need to ensure that our organizations continue to operate at some minimum acceptable threshold capacity and quickly bounce back to full productivity.

Business continuity (BC) is an organization's ability to maintain business functions or quickly resume them in the event that risks are realized and result in disruptions. The events can be pretty mundane, such as a temporary power outage, loss of network connectivity, or a critical employee (such as a systems administrator) suddenly becoming ill. These events could also be major disasters, such as an earthquake, explosion, or energy grid failure. *Disaster recovery (DR)*, by contrast to BC, is the process of minimizing the effects of a disaster or major disruption. It means taking the necessary steps to ensure that the resources, personnel, and business processes are safe and able to resume operation in a timely manner. So, DR is part of BC and the *disaster recovery plan (DRP)* covers a subset of events compared to the broader *business continuity plan (BCP)*.



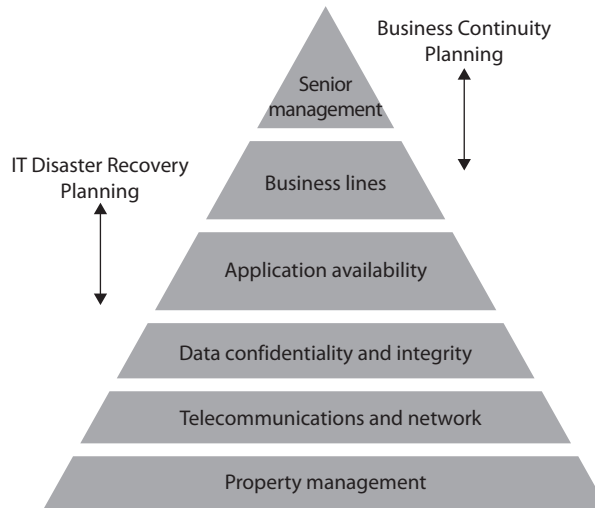
EXAM TIP A business continuity plan (BCP) and a disaster recovery plan (DRP) are related but different. The DRP is a subset of the BCP and is focused on the immediate aftermath of a disaster. The BCP is much broader and covers any disruption including (but not limited to) disasters.



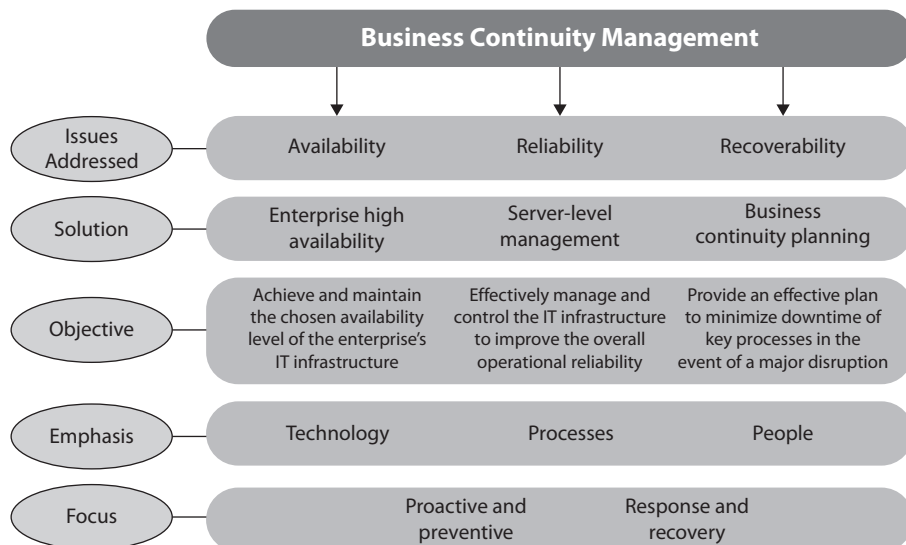
NOTE We discuss disaster recovery plans in detail in Chapter 23.

A BCP can include getting critical systems to another environment while repair of the original facilities is underway, getting the right people to the right places during this time, and performing business in a different mode until regular conditions are back in place. A BCP also involves dealing with customers, partners, and shareholders through different channels until everything returns to normal. So, disaster recovery deals with,

“Oh my goodness, the sky is falling,” and continuity planning deals with, “Okay, the sky fell. Now, how do we stay in business until someone can put the sky back where it belongs?”



While disaster recovery and business continuity planning are directed at the development of plans, *business continuity management (BCM)* is the holistic management process that should cover both of them. BCM provides a framework for integrating resilience with the capability for effective responses in a manner that protects the interests of an organization’s key stakeholders. The main objective of BCM is to allow the organization to continue to perform business operations under various conditions.



Certain characteristics run through many of the chapters in this book: availability, integrity, and confidentiality. Here, we point out that integrity and confidentiality must be considered not only in everyday procedures but also in those procedures undertaken immediately after a disaster or disruption. For instance, it may not be appropriate to leave a server that holds confidential information in one building while everyone else moves to another building. Equipment that provides secure VPN connections may be destroyed and the team might respond by focusing on enabling remote access functionality while forgetting about the needs of encryption. In most situations the organization is purely focused on getting back up and running, thus focusing on functionality. If security is not integrated and implemented properly, the effects of the physical disaster can be amplified as threat actors come in and steal sensitive information. Many times an organization is much more vulnerable *after* a disaster hits, because the security services used to protect it may be unavailable or operating at a reduced capacity. Therefore, it is important that if the organization has secret stuff, it stays secret.

Availability is one of the main themes behind business continuity planning, in that it ensures that the resources required to keep the business going will continue to be available to the people and systems that rely upon them. This may mean backups need to be done religiously and that redundancy needs to be factored into the architecture of the systems, networks, and operations. If communication lines are disabled or if a service is rendered unusable for any significant period of time, there must be a quick and tested way of establishing alternative communications and services. We will be diving into the many ways organizations can implement availability solutions for continuity and recovery purposes throughout this section.

When looking at business continuity planning, some organizations focus mainly on backing up data and providing redundant hardware. Although these items are extremely important, they are just small pieces of the organization's overall operations pie. Hardware and computers need people to configure and operate them, and data is usually not useful unless it is accessible by other systems and possibly outside entities. Thus, a larger picture

Business Continuity Planning

Preplanned procedures allow an organization to

- Provide an immediate and appropriate response to emergency situations
- Protect lives and ensure safety
- Reduce business impact
- Resume critical business functions
- Work with outside vendors and partners during the recovery period
- Reduce confusion during a crisis
- Ensure survivability of the organization
- Get “up and running” quickly after a disaster

of how the various processes within an organization work together needs to be understood. Planning must include getting the right people to the right places, documenting the necessary configurations, establishing alternative communications channels (voice and data), providing power, and making sure all dependencies are properly understood and taken into account.

It is also important to understand how automated tasks can be carried out manually, if necessary, and how business processes can be safely altered to keep the operation of the organization going. This may be critical in ensuring the organization survives the event with the least impact to its operations. Without this type of vision and planning, when a disaster hits, an organization could have its backup data and redundant servers physically available at the alternative facility, but the people responsible for activating them may be standing around in a daze, not knowing where to start or how to perform in such a different environment.

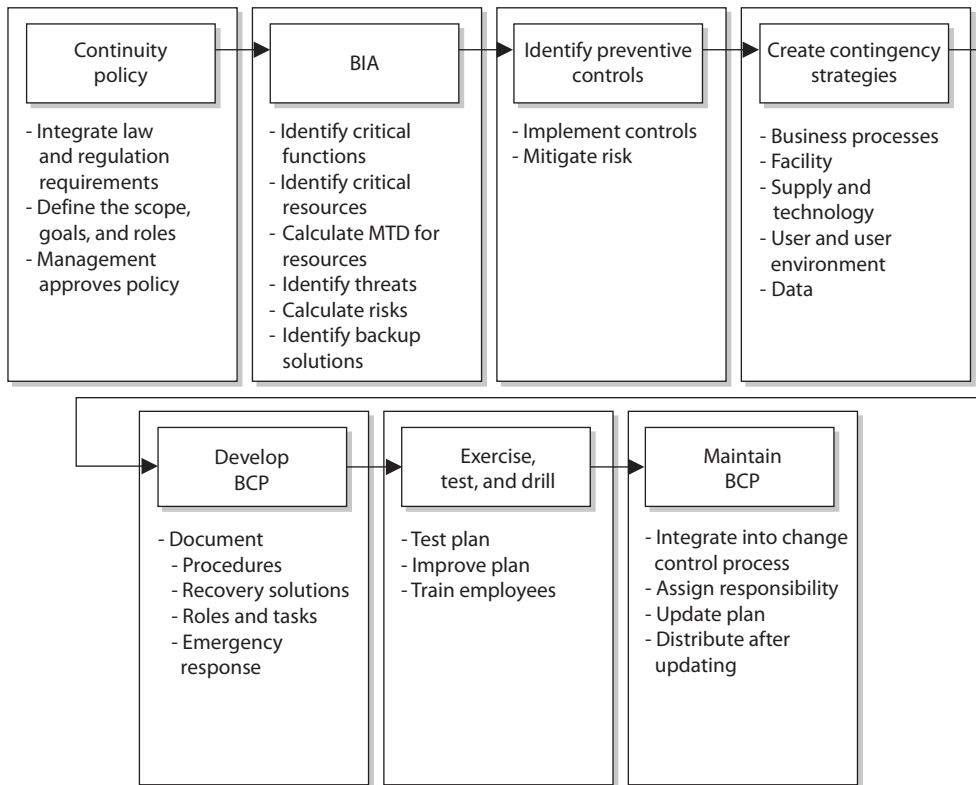
Standards and Best Practices

Although no specific scientific equation must be followed to create continuity plans, certain best practices have proven themselves over time. The National Institute of Standards and Technology is responsible for developing best practices and standards as they pertain to U.S. government and military environments. It is common for NIST to document the requirements for these types of environments, and then everyone else in the industry uses NIST's documents as guidelines. So these are "musts" for U.S. government organizations and "good to have" for other, nongovernment entities.

NIST outlines the following steps in SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*:

1. *Develop the continuity planning policy statement.* Write a policy that provides the guidance necessary to develop a BCP and that assigns authority to the necessary roles to carry out these tasks.
2. *Conduct the business impact analysis (BIA).* Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities and threats, and calculate risks.
3. *Identify preventive controls.* Once threats are recognized, identify and implement controls and countermeasures to reduce the organization's risk level in an economical manner.
4. *Create contingency strategies.* Formulate methods to ensure systems and critical functions can be brought online quickly.
5. *Develop an information system contingency plan.* Write procedures and guidelines for how the organization can still stay functional in a crippled state.
6. *Ensure plan testing, training, and exercises.* Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.
7. *Ensure plan maintenance.* Put in place steps to ensure the BCP is a living document that is updated regularly.

Although NIST SP 800-34 deals specifically with IT contingency plans, these steps are similar when creating enterprise-wide BCPs and BCM programs.



Since BCM is so critical, it is actually addressed by other standards-based organizations, listed here:

ISO/IEC 27031:2011 Guidelines for information and communications technology readiness for business continuity. This ISO/IEC standard is a component of the overall ISO/IEC 27000 series.

ISO 22301:2019 International standard for business continuity management systems. The specification document against which organizations will seek certification.

Business Continuity Institute's Good Practice Guidelines (GPG) Represents the consensus view of an international group of BC practitioners. As of this writing, the latest edition was published in 2018. It is organized around six Professional Practices (PP):

- **Policy and Program Management (PP1)** Focuses on governance
- **Embedding Business Continuity (PP2)** Provides guidance on embedding BCM in the organization's culture, which includes awareness and training

- **Analysis (PP3)** Addresses organizational review, risk assessment, and business impact analysis, among other topics
- **Design (PP4)** Focuses on identifying and selecting the right BC solutions
- **Implementation (PP5)** Addresses what should go into the BC plan
- **Validation (PP6)** Covers exercising, maintaining, and reviewing the program

DRI International Institute's Professional Practices for Business Continuity Management Best practices and framework to allow for BCM processes, which are broken down into the following sections:

- Program Initiation and Management
- Risk Assessment
- Business Impact Analysis
- Business Continuity Strategies
- Incident Response
- Plan Development and Implementation
- Awareness and Training Programs
- Business Continuity Plan Exercise, Assessment, and Maintenance
- Crisis Communications
- Coordination with External Agencies

Why are there so many sets of best practices and which is the best for your organization? If your organization is part of the U.S. government or a government contracting organization, then you need to comply with the NIST standards. If your organization is in Europe or your organization does business with other organizations in Europe, then you might need to follow the European Union Agency for Cybersecurity (ENISA) requirements. While we are not listing all of them here, there are other country-based BCM standards that your organization might need to comply with if it is residing in or does business in one of those specific countries. If your organization needs to get ISO certified, then ISO/IEC 27031 and ISO 22301 could be the standards to follow. While the first of these is focused on IT, the second is broader in scope and addresses the needs of the entire organization.

Making BCM Part of the Enterprise Security Program

As we already explained, every organization should have security policies, procedures, standards, and guidelines. People who are new to information security commonly think that this is one pile of documentation that addresses all issues pertaining to security, but it is more complicated than that—of course.

Business continuity planning ought to be fully integrated into the organization as a regular management process, just like auditing or strategic planning or other “normal”

Understanding the Organization First

An organization has no real hope of rebuilding itself and its processes after a disaster if it does not have a good understanding of how its organization works in the first place. This notion might seem absurd at first. You might think, “Well, of course an organization knows how it works.” But you would be surprised at how difficult it is to fully understand an organization down to the level of detail required to rebuild it. Each individual may know and understand his or her little world within the organization, but hardly anyone at any organization can fully explain how each and every business process takes place.

processes. Instead of being considered an outsider, BCP should be “part of the team.” Further, final responsibility for BCP should belong not to the BCP team or its leader, but to a high-level executive manager, preferably a member of the executive board. This will reinforce the image and reality of continuity planning as a function seen as vital to the organizational chiefs.

By analyzing and planning for potential disruptions to the organization, the BCP team can assist other business disciplines in their own efforts to effectively plan for and respond effectively and with resilience to emergencies. Given that the ability to respond depends on operations and management personnel throughout the organization, such capability should be developed organization-wide. It should extend throughout every location of the organization and up the employee ranks to top-tier management.

As such, the BCP program needs to be a living entity. As an organization goes through changes, so should the program, thereby ensuring it stays current, usable, and effective. When properly integrated with change management processes, the program stands a much better chance of being continually updated and improved upon. Business continuity is a foundational piece of an effective security program and is critical to ensuring relevance in time of need.

A very important question to ask when first developing a BCP is *why* it is being developed. This may seem silly and the answer may at first appear obvious, but that is not always the case. You might think that the reason to have these plans is to deal with an unexpected disaster and to get people back to their tasks as quickly and as safely as possible, but the full story is often a bit different. Why are most companies in business? To make money and be profitable. If these are usually the main goals of businesses, then any BCP needs to be developed to help achieve and, more importantly, maintain these goals. The main reason to develop these plans in the first place is to reduce the risk of financial loss by improving the company’s ability to recover and restore operations. This encompasses the goals of mitigating the effects of the disaster.

Not all organizations are businesses that exist to make profits. Government agencies, military units, nonprofit organizations, and the like exist to provide some type of protection or service to a nation or society. Whereas a company must create its BCP to ensure that revenue continues to come in so that the company can stay in business,

other types of organizations must create their BCPs to make sure they can still carry out their critical tasks. Although the focus and business drivers of the organizations and companies may differ, their BCPs often have similar constructs—which is to get their critical processes up and running.

Protecting what is most important to a company is rather difficult if what is most important is not first identified. Senior management is usually involved with this step because it has a point of view that extends beyond each functional manager's focus area of responsibility. Senior management has the visibility needed to establish the scope of the plan. The company's BCP should be focused on the company's critical mission and business functions. And, conversely, the BCP must support the organization's overall strategy. The functions must have priorities set upon them to indicate which is most crucial to a company's survival. The scope of the BCP is defined by which of these functions are considered important enough to warrant the investment of resources required for BC.

As stated previously, for many companies, financial operations are most critical. As an example, an automotive company would be affected far more seriously if its credit and loan services were unavailable for a day than if, say, an assembly line went down for a day, since credit and loan services are where it generates the biggest revenues. For other organizations, customer service might be the most critical area to ensure that order processing is not negatively affected. For example, if a company makes heart pacemakers and its physician services department is unavailable at a time when an operating room surgeon needs to contact it because of a complication, the results could be disastrous for the patient. The surgeon and the company would likely be sued, and the company would likely never again be able to sell another pacemaker to that surgeon, her colleagues, or perhaps even the patient's health maintenance organization (HMO). It would be very difficult to rebuild reputation and sales after something like that happened.

Advanced planning for emergencies covers issues that were thought of and foreseen. Many other problems may arise that are not covered in the BCP; thus, flexibility in the plan is crucial. The plan is a systematic way of providing a checklist of actions that should take place right after a disaster. These actions have been thought through to help the people involved be more efficient and effective in dealing with traumatic situations.

The most critical part of establishing and maintaining a current BCP is management support. Management must be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support. The business case may include current vulnerabilities, regulatory and legal obligations, the current status of recovery plans, and recommendations. Management is mostly concerned with cost/benefit issues, so preliminary numbers need to be gathered and potential losses estimated. A cost/benefit analysis should include shareholder, stakeholder, regulatory, and legislative impacts, as well as impacts on products, services, and personnel. The decision of how a company should recover is commonly a business decision and should always be treated as such.

Business Impact Analysis

Business continuity planning deals with uncertainty and chance. What is important to note here is that even though you cannot predict whether or when a disaster will happen,

that doesn't mean you can't plan for it. Just because we are not planning for an earthquake to hit us tomorrow morning at 10 A.M. doesn't mean we can't plan the activities required to successfully survive when an earthquake (or a similar disaster) does hit. The point of making these plans is to try to think of all the possible disasters that could take place, estimate the potential damage and loss, categorize and prioritize the potential disasters, and develop viable alternatives in case those events do actually happen.

A *business impact analysis (BIA)* is considered a *functional analysis*, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level. But how do we determine a classification scheme based on criticality levels?

The BCP committee must identify the threats to the organization and map them to the following characteristics:

- Maximum tolerable downtime and disruption for activities
- Operational disruption and productivity
- Financial considerations
- Regulatory responsibilities
- Reputation

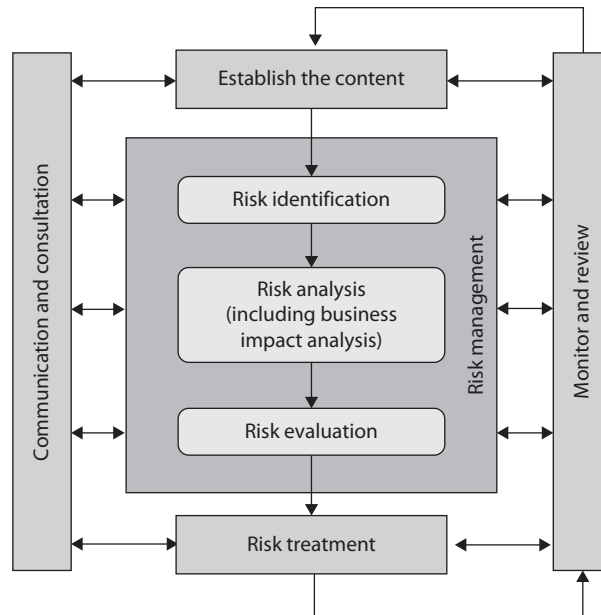
The committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know—department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks—whether processes, transactions, or services, along with any relevant dependencies—get accomplished within the organization. The team should build process flow diagrams, which will be used throughout the BIA and plan development stages.

Upon completion of the data collection phase, the BCP committee needs to conduct a BIA to establish which processes, devices, or operational activities are critical. If a system stands on its own, doesn't affect other systems, and is of low criticality, then it can be classified as a tier-two or tier-three recovery step. This means these resources will not be dealt with during the recovery stages until the most critical (tier one) resources are up and running. This analysis can be completed using a standard risk assessment as illustrated in Figure 2-9.

Risk Assessment

To achieve success, the organization should systematically plan and execute a formal BCP-related risk assessment. The assessment fully takes into account the organization's

Figure 2-9
Risk assessment
process



tolerance for continuity risks. The risk assessment also makes use of the data in the BIA to supply a consistent estimate of exposure.

As indicators of success, the risk assessment should identify, evaluate, and record all relevant items, which may include

- Vulnerabilities for all of the organization's most time-sensitive resources and activities
- Threats and hazards to the organization's most urgent resources and activities
- Measures that cut the possibility, length, or effect of a disruption on critical services and products
- Single points of failure; that is, concentrations of risk that threaten business continuity
- Continuity risks from concentrations of critical skills or critical shortages of skills
- Continuity risks due to outsourced vendors and suppliers
- Continuity risks that the BCP program has accepted, that are handled elsewhere, or that the BCP program does not address

Risk Assessment Evaluation and Process

In a BCP setting, a risk assessment looks at the impact and likelihood of various threats that could trigger a business disruption. The tools, techniques, and methods of risk assessment include determining threats, assessing probabilities, tabulating threats, and analyzing costs and benefits.

The end goals of a business continuity–focused risk assessment include

- Identifying and documenting single points of failure
- Making a prioritized list of threats to the particular business processes of the organization
- Putting together information for developing a management strategy for risk control and for developing action plans for addressing risks
- Documenting acceptance of identified risks, or documenting acknowledgment of risks that will not be addressed

The risk assessment is assumed to take the form of the equation $\text{Risk} = \text{Threat} \times \text{Impact} \times \text{Probability}$. However, the BIA adds the dimension of time to this equation. In other words, risk mitigation measures should be geared toward those things that might most rapidly disrupt critical business processes and commercial activities.

The main parts of a risk assessment are

- Review the existing strategies for risk management
- Construct a numerical scoring system for probabilities and impacts
- Make use of a numerical score to gauge the effect of the threat
- Estimate the probability of each threat
- Weigh each threat through the scoring system
- Calculate the risk by combining the scores of likelihood and impact of each threat
- Get the organization's sponsor to sign off on these risk priorities
- Weigh appropriate measures
- Make sure that planned measures that alleviate risk do not heighten other risks
- Present the assessment's findings to executive management

Threats can be man-made, natural, or technical. A man-made threat may be an arsonist, a terrorist, or a simple mistake that can have serious outcomes. Natural threats may be tornadoes, floods, hurricanes, or earthquakes. Technical threats may be data corruption, loss of power, device failure, or loss of a data communications line. It is important to identify all possible threats and estimate the probability of them happening. Some issues may not immediately come to mind when developing these plans, such as an employee strike, vandals, disgruntled employees, or hackers, but they do need to be identified. These issues are often best addressed in a group with scenario-based exercises. This ensures that if a threat becomes reality, the plan includes the ramifications on *all* business tasks, departments, and critical operations. The more issues that are thought of and planned for, the better prepared an organization will be if and when these events take place.

The BCP committee needs to step through scenarios in which the following problems result:

- Equipment malfunction or unavailable equipment
- Unavailable utilities (HVAC, power, communications lines)
- Facility becomes unavailable
- Critical personnel become unavailable
- Vendor and service providers become unavailable
- Software and/or data corruption

The specific scenarios and damage types can vary from organization to organization.

Assigning Values to Assets

Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. The goal is to see exactly how an organization will be affected by different threats. The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the organization to ensure that the findings are appropriate and that it describes the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts.

Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

- Loss in reputation and public confidence
- Loss of competitive advantages

BIA Steps

The more detailed and granular steps of a BIA are outlined here:

1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the organization's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

We cover each of these steps in this chapter.

- Increase in operational expenses
- Violations of contract agreements
- Violations of legal and regulatory requirements
- Delayed-income costs
- Loss in revenue
- Loss in productivity

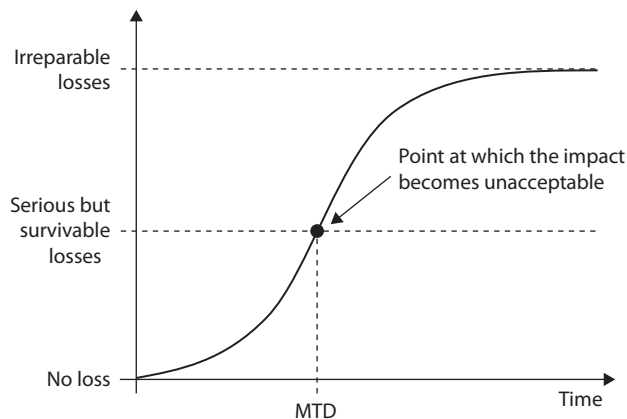
These costs can be direct or indirect and must be properly accounted for.

For instance, if the BCP team is looking at the threat of a terrorist bombing, it is important to identify which business function most likely would be targeted, how all business functions could be affected, and how each bulleted item in the loss criteria would be directly or indirectly involved. The timeliness of the recovery can be critical for business processes and the company's survival. For example, it may be acceptable to have the customer-support functionality out of commission for two days, whereas five days may leave the company in financial ruin.

After identifying the critical functions, it is necessary to find out exactly what is required for these individual business processes to take place. The resources that are required for the identified business processes are not necessarily just computer systems, but may include personnel, procedures, tasks, supplies, and vendor support. It must be understood that if one or more of these support mechanisms is not available, the critical function may be doomed. The team must determine what type of effect unavailable resources and systems will have on these critical functions.

The BIA identifies which of the organization's critical systems are needed for survival and estimates the outage time that can be tolerated by the organization as a result of various unfortunate events. The outage time that can be endured by an organization is referred to as the *maximum tolerable downtime (MTD)* or *maximum tolerable period of disruption (MTPD)*, which is illustrated in Figure 2-10.

Figure 2-10
Maximum
tolerable
downtime



The following are some MTD estimates that an organization may use. Note that these are sample estimates that will vary from organization to organization and from business unit to business unit.

- **Nonessential** 30 days
- **Normal** 7 days
- **Important** 72 hours
- **Urgent** 24 hours
- **Critical** Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the organization can survive without it. These estimates will help the organization determine what backup solutions are necessary to ensure the availability of these resources. The shorter the MTD, the higher priority of recovery for the function in question. Thus, the items classified as Urgent should be addressed before those classified as Normal.

For example, if being without a T1 communication line for three hours would cost the company \$130,000, the T1 line could be considered Critical, and thus the company should put in a backup T1 line from a different carrier. If a server going down and being unavailable for ten days will only cost the company \$250 in revenue, this would fall into the Normal category, and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor's SLA, which may promise to have it back online in eight days.

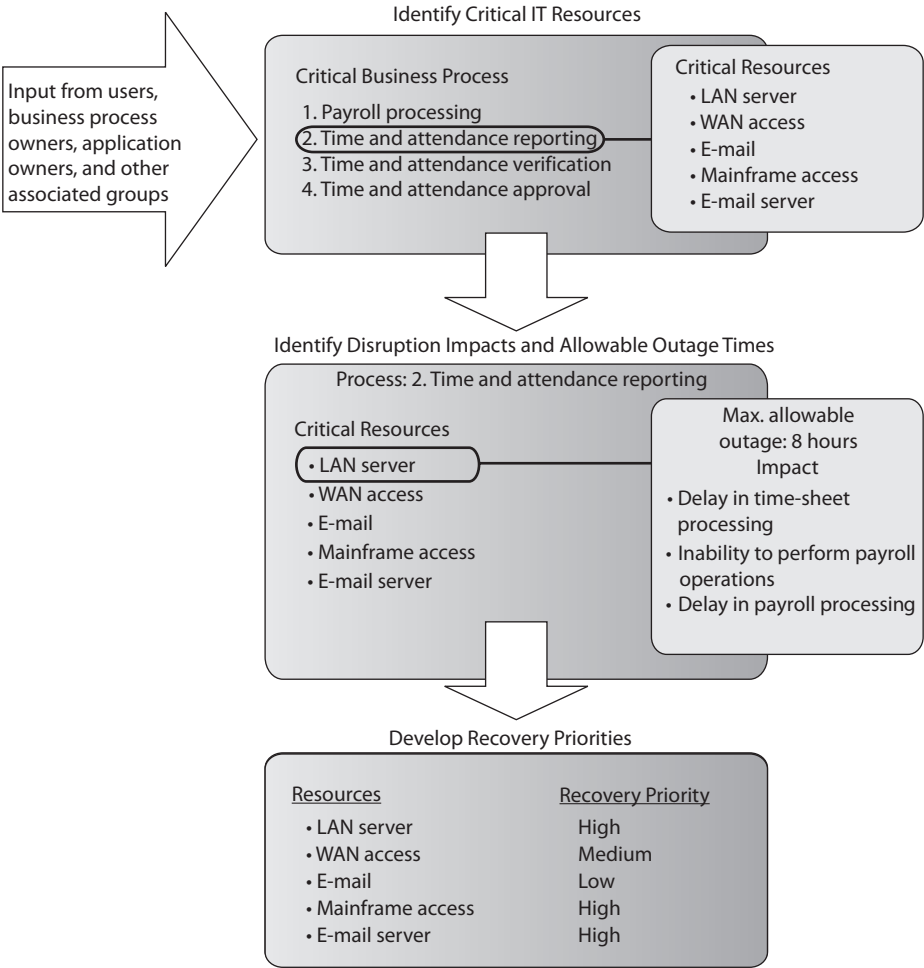
Sometimes the MTD will depend in large measure on the type of organization in question. For instance, a call center—a vital link to current and prospective clients—will have a short MTD, perhaps measured in minutes instead of weeks. A common solution is to split up the calls through multiple call centers placed in differing locales. If one call center is knocked out of service, the other one can temporarily pick up the load. Manufacturing can be handled in various ways. Examples include subcontracting the making of products to an outside vendor, manufacturing at multiple sites, and warehousing an extra supply of products to fill gaps in supply in case of disruptions to normal manufacturing.

The BCP team must try to think of all possible events that might occur that could turn out to be detrimental to an organization. The BCP team also must understand it cannot possibly contemplate all events, and thus protection may not be available for every scenario introduced. Being properly prepared specifically for a flood, earthquake, terrorist attack, or lightning strike is not as important as being properly prepared to respond to *anything* that damages or disrupts critical business functions.

All of the previously mentioned disasters could cause these results, but so could a meteor strike, a tornado, or a wing falling off a plane passing overhead. So the moral of the story is to be prepared for the loss of any or all business resources, instead of focusing on the events that could cause the loss.



EXAM TIP A BIA is performed at the beginning of business continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the organization’s critical systems needed for survival and estimates the outage time that can be tolerated by the organization as a result of a disaster or disruption.



Chapter Review

We took a very detailed look at the way in which we manage risk to our information systems. We know that no system is truly secure, so our job is to find the most likely and the most dangerous threat actions so that we can address them first. The process of quantifying losses and their probabilities of occurring is at the heart of risk assessments. Armed with that information, we are able to make good decisions in terms of controls, processes, and costs. Our approach is focused not solely on the human adversary but also on any source of loss to our organizations. Most importantly, we use this information to devise ways in which to ensure we can continue business operations in the face of any reasonable threat.

Quick Review

- Risk management is the process of identifying and assessing risk, reducing it to an acceptable level, and ensuring it remains at that level.
- An information systems risk management (ISRM) policy provides the foundation and direction for the organization's security risk management processes and procedures and should address all issues of information security.
- A threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.
- Four risk assessment methodologies with which you should be familiar are NIST SP 800-30; Facilitated Risk Analysis Process (FRAP); Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE); and Failure Modes and Effect Analysis (FMEA).
- Failure Modes and Effect Analysis (FMEA) is a method for determining functions, identifying functional failures, and assessing the causes of failure and their effects through a structured process.
- A fault tree analysis is a useful approach to detect failures that can take place within complex environments and systems.
- A quantitative risk analysis attempts to assign monetary values to components within the analysis.
- A purely quantitative risk analysis is not possible because qualitative items cannot be quantified with precision.
- Qualitative risk analysis uses judgment and intuition instead of numbers.
- Qualitative risk analysis involves people with the requisite experience and education evaluating threat scenarios and rating the probability, potential loss, and severity of each threat based on their personal experience.
- $\text{Single loss expectancy} \times \text{frequency per year} = \text{annualized loss expectancy}$
($\text{SLE} \times \text{ARO} = \text{ALE}$)

- The main goals of risk analysis are the following: identify assets and assign values to them, identify vulnerabilities and threats, quantify the impact of potential threats, and provide an economic balance between the impact of the risk and the cost of the safeguards.
- Capturing the degree of uncertainty when carrying out a risk analysis is important, because it indicates the level of confidence the team and management should have in the resulting figures.
- Automated risk analysis tools reduce the amount of manual work involved in the analysis. They can be used to estimate future expected losses and calculate the benefits of different security measures.
- The risk management team should include individuals from different departments within the organization, not just technical personnel.
- Risk can be transferred, avoided, reduced, or accepted.
- $\text{Threats} \times \text{vulnerability} \times \text{asset value} = \text{total risk}$.
- $(\text{Threats} \times \text{vulnerability} \times \text{asset value}) \times \text{controls gap} = \text{residual risk}$.
- When choosing the right safeguard to reduce a specific risk, the cost, functionality, and effectiveness must be evaluated and a cost/benefit analysis performed.
- There are three main categories of controls: administrative, technical, and physical.
- Controls can also be grouped by types, depending on their intended purpose, as preventive, detective, corrective, deterrent, recovery, and compensating.
- A control assessment is an evaluation of one or more controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome.
- Security control verification answers the question “did we implement the control right?” while validation answers the question “did we implement the right control?”
- Risk monitoring is the ongoing process of adding new risks, reevaluating existing ones, removing moot ones, and continuously assessing the effectiveness of your controls at mitigating all risks to tolerable levels.
- Change management processes deal with monitoring changes to your environment and dealing with the risks they could introduce.
- Continuous improvement is the practice of identifying opportunities, mitigating threats, improving quality, and reducing waste as an ongoing effort. It is the hallmark of mature and effective organizations.
- A supply chain is a sequence of suppliers involved in delivering some product.
- Business continuity management (BCM) is the overarching approach to managing all aspects of BCP and DRP.
- A business continuity plan (BCP) contains strategy documents that provide detailed procedures that ensure critical business functions are maintained and that help minimize losses of life, operations, and systems.

- A BCP provides procedures for emergency responses, extended backup operations, and post-disaster recovery.
- A BCP should have an enterprise-wide reach, with each individual organizational unit having its own detailed continuity and contingency plans.
- A BCP needs to prioritize critical applications and provide a sequence for efficient recovery.
- A BCP requires senior executive management support for initiating the plan and final approval.
- BCPs can quickly become outdated due to personnel turnover, reorganizations, and undocumented changes.
- Executives may be held liable if proper BCPs are not developed and used.
- Threats can be natural, man-made, or technical.
- The business impact analysis (BIA) is one of the most important first steps in the planning development. Qualitative and quantitative data on the business impact of a disaster need to be gathered, analyzed, interpreted, and presented to management.
- Executive commitment and support are the most critical elements in developing the BCP.
- A business case must be presented to gain executive support. This is done by explaining regulatory and legal requirements, exposing vulnerabilities, and providing solutions.
- Plans should be prepared by the people who will actually carry them out.
- The planning group should comprise representatives from all departments or organizational units.
- The BCP team should identify the individuals who will interact with external players, such as the reporters, shareholders, customers, and civic officials. Response to the disaster should be done quickly and honestly, and should be consistent with any other organizational response.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. When is it acceptable to not take action on an identified risk?
 - A. Never. Good security addresses and reduces all risks.
 - B. When political issues prevent this type of risk from being addressed.
 - C. When the necessary countermeasure is complex.
 - D. When the cost of the countermeasure outweighs the value of the asset and potential loss.

2. Which is the most valuable technique when determining if a specific security control should be implemented?
 - A. Risk analysis
 - B. Cost/benefit analysis
 - C. ALE results
 - D. Identifying the vulnerabilities and threats causing the risk
3. Which best describes the purpose of the ALE calculation?
 - A. Quantifies the security level of the environment
 - B. Estimates the loss possible for a countermeasure
 - C. Quantifies the cost/benefit result
 - D. Estimates the loss potential of a threat in a span of a year
4. How do you calculate residual risk?
 - A. Threats \times risks \times asset value
 - B. (Threats \times asset value \times vulnerability) \times risks
 - C. SLE \times frequency = ALE
 - D. (Threats \times vulnerability \times asset value) \times controls gap
5. Why should the team that will perform and review the risk analysis information be made up of people in different departments?
 - A. To make sure the process is fair and that no one is left out.
 - B. It shouldn't. It should be a small group brought in from outside the organization because otherwise the analysis is biased and unusable.
 - C. Because people in different departments understand the risks of their department. Thus, it ensures the data going into the analysis is as close to reality as possible.
 - D. Because the people in the different departments are the ones causing the risks, so they should be the ones held accountable.
6. Which best describes a quantitative risk analysis?
 - A. A scenario-based analysis to research different security threats
 - B. A method used to apply severity levels to potential loss, probability of loss, and risks
 - C. A method that assigns monetary values to components in the risk assessment
 - D. A method that is based on gut feelings and opinions
7. Why is a truly quantitative risk analysis not possible to achieve?
 - A. It is possible, which is why it is used.
 - B. It assigns severity levels. Thus, it is hard to translate into monetary values.
 - C. It is dealing with purely quantitative elements.
 - D. Quantitative measures must be applied to qualitative elements.

Use the following scenario to answer Questions 9–11. A company has an e-commerce website that carries out 60 percent of its annual revenue. Under the current circumstances, the annualized loss expectancy for a website against the threat of attack is \$92,000. After implementing a new application-layer firewall, the new ALE would be \$30,000. The firewall costs \$65,000 per year to implement and maintain.

8. How much does the firewall save the company in loss expenses?
 - A. \$62,000
 - B. \$3,000
 - C. \$65,000
 - D. \$30,000
9. What is the value of the firewall to the company?
 - A. \$62,000
 - B. \$3,000
 - C. –\$62,000
 - D. –\$3,000
10. Which of the following describes the company's approach to risk management?
 - A. Risk transference
 - B. Risk avoidance
 - C. Risk acceptance
 - D. Risk mitigation

Use the following scenario to answer Questions 11–13. A small remote office for a company is valued at \$800,000. It is estimated, based on historical data, that a fire is likely to occur once every ten years at a facility in this area. It is estimated that such a fire would destroy 60 percent of the facility under the current circumstances and with the current detective and preventive controls in place.

11. What is the single loss expectancy (SLE) for the facility suffering from a fire?
 - A. \$80,000
 - B. \$480,000
 - C. \$320,000
 - D. 60%
12. What is the annualized rate of occurrence (ARO)?
 - A. 1
 - B. 10
 - C. .1
 - D. .01

13. What is the annualized loss expectancy (ALE)?
 - A. \$480,000
 - B. \$32,000
 - C. \$48,000
 - D. .6
14. Which of the following is not one of the three key areas for risk monitoring?
 - A. Threat
 - B. Effectiveness
 - C. Change
 - D. Compliance
15. What is one of the first steps in developing a business continuity plan?
 - A. Identify a backup solution.
 - B. Perform a simulation test.
 - C. Perform a business impact analysis.
 - D. Develop a business resumption plan.

Answers

1. **D.** Organizations may decide to live with specific risks they are faced with if the cost of trying to protect themselves would be greater than the potential loss if the threat were to become real. Countermeasures are usually complex to a degree, and there are almost always political issues surrounding different risks, but these are not reasons to not implement a countermeasure.
2. **B.** Although the other answers may seem correct, B is the best answer here. This is because a risk analysis is performed to identify risks and come up with suggested countermeasures. The annualized loss expectancy (ALE) tells the organization how much it could lose if a specific threat became real. The ALE value will go into the cost/benefit analysis, but the ALE does not address the cost of the countermeasure and the benefit of a countermeasure. All the data captured in answers A, C, and D is inserted into a cost/benefit analysis.
3. **D.** The ALE calculation estimates the potential loss that can affect one asset from a specific threat within a one-year time span. This value is used to figure out the amount of money that should be earmarked to protect this asset from this threat.
4. **D.** The equation is more conceptual than practical. It is hard to assign a number to an individual vulnerability or threat. This equation enables you to look at the potential loss of a specific asset, as well as the controls gap (what the specific countermeasure cannot protect against). What remains is the residual risk, which is what is left over after a countermeasure is implemented.

5. **C.** An analysis is only as good as the data that goes into it. Data pertaining to risks the organization faces should be extracted from the people who understand best the business functions and environment of the organization. Each department understands its own threats and resources, and may have possible solutions to specific threats that affect its part of the organization.
6. **C.** A quantitative risk analysis assigns monetary values and percentages to the different components within the assessment. A qualitative analysis uses opinions of individuals and a rating system to gauge the severity level of different threats and the benefits of specific countermeasures.
7. **D.** During a risk analysis, the team is trying to properly predict the future and all the risks that future may bring. It is somewhat of a subjective exercise and requires educated guessing. It is very hard to properly predict that a flood will take place once in ten years and cost a company up to \$40,000 in damages, but this is what a quantitative analysis tries to accomplish.
8. **A.** \$62,000 is the correct answer. The firewall reduced the annualized loss expectancy (ALE) from \$92,000 to \$30,000 for a savings of \$62,000. The formula for ALE is $\text{single loss expectancy} \times \text{annualized rate of occurrence} = \text{ALE}$. Subtracting the ALE value after the firewall is implemented from the value before it was implemented results in the potential loss savings this type of control provides.
9. **D.** $-\$3,000$ is the correct answer. The firewall saves \$62,000, but costs \$65,000 per year. $62,000 - 65,000 = -3,000$. The firewall actually costs the company more than the original expected loss, and thus the value to the company is a negative number. The formula for this calculation is $(\text{ALE before the control is implemented}) - (\text{ALE after the control is implemented}) - (\text{annual cost of control}) = \text{value of control}$.
10. **D.** Risk mitigation involves employing controls in an attempt to reduce either the likelihood or damage associated with an incident, or both. The four ways of dealing with risk are accept, avoid, transfer, and mitigate (reduce). A firewall is a countermeasure installed to reduce the risk of a threat.
11. **B.** \$480,000 is the correct answer. The formula for single loss expectancy (SLE) is $\text{asset value} \times \text{exposure factor (EF)} = \text{SLE}$. In this situation the formula would work out as $\text{asset value} (\$800,000) \times \text{exposure factor (60\%)} = \$480,000$. This means that the company has a potential loss value of \$480,000 pertaining to this one asset (facility) and this one threat type (fire).
12. **C.** The annualized rate occurrence (ARO) is the frequency that a threat will most likely occur within a 12-month period. It is a value used in the ALE formula, which is $\text{SLE} \times \text{ARO} = \text{ALE}$.
13. **C.** \$48,000 is the correct answer. The annualized loss expectancy formula ($\text{SLE} \times \text{ARO} = \text{ALE}$) is used to calculate the loss potential for one asset experiencing one threat in a 12-month period. The resulting ALE value helps to determine the amount that can reasonably be spent in the protection of that asset. In this situation, the company should not spend over \$48,000 on protecting this

asset from the threat of fire. ALE values help organizations rank the severity level of the risks they face so they know which ones to deal with first and how much to spend on each.

14. **A.** Risk monitoring activities should be focused on three key areas: effectiveness, change, and compliance. Changes to the threat landscape should be incorporated directly into the first two, and indirectly into compliance monitoring.
15. **C.** A business impact analysis includes identifying critical systems and functions of an organization and interviewing representatives from each department. Once management's support is solidified, a BIA needs to be performed to identify the threats the company faces and the potential costs of these threats.

This page intentionally left blank

Compliance

This chapter presents the following:

- Regulations, laws, and crimes involving computers
- Intellectual property
- Data breaches
- Compliance requirements
- Investigations

If you think compliance is expensive, try noncompliance.

—Paul McNulty

Rules, formal or otherwise, are essential for prosperity in any context. This is particularly true when it comes to cybersecurity. Even if our adversaries don't follow the rules (and clearly they don't), we must understand the rules that apply to us and follow them carefully. In this chapter, we discuss the various laws and regulations that deal with computer information systems. We can't really address each piece of legislation around the world, since that would take multiple books longer than this one. However, we will offer as examples some of the most impactful laws and regulations affecting multinational enterprises. These include laws and regulations applicable to cybercrimes, privacy, and intellectual property, among others. The point of this chapter is not to turn you into a cyberlaw expert, but to make you aware of some of the topics about which you should have conversations with your legal counsel and compliance colleagues as you develop and mature your cybersecurity program.

Laws and Regulations

Before we get into the details of what you, as a cybersecurity leader, are required to do, let's start by reviewing some foundational concepts about what laws and regulations are, exploring how they vary around the world, and then putting them into a holistic context.

Law is a system of rules created by either a government or a society, recognized as binding by that group, and enforced by some specific authority. Laws apply equally to everyone in the country or society. It is important to keep in mind that laws are not always written down and may be customary, as discussed shortly. *Regulations*, by contrast, are written rules dealing with specific details or procedures, issued by an executive body

and having the force of law. Regulations apply only to the specific entities that fall under the authority of the agency that issues them. So, while any U.S.-based organization is subject to a U.S. law called the Computer Fraud and Abuse Act (CFAA), only U.S. organizations that deal with data concerning persons in the European Union (EU) would also be subject to the General Data Protection Regulation (GDPR).

Types of Legal Systems

Your organization may be subject to laws and regulations from multiple jurisdictions. As just mentioned, if your organization is based in the United States but handles data of citizens of the EU, your organization is subject to both the CFAA and the GDPR. It is important to keep in mind that different countries can have very different legal systems. Your legal department will figure out jurisdictions and applicability, but you need to be aware of what this disparity of legal systems means to your cybersecurity program. To this end, it is helpful to become familiar with the major legal systems you may come across. In this section, we cover the core components of the various legal systems and what differentiates them.

Civil (Code) Law System

- System of law used in continental European countries such as France and Spain.
- Different legal system from the common law system used in the United Kingdom and United States.
- Civil law system is rule-based law, not precedent-based.
- For the most part, a civil law system is focused on codified law—or written laws.
- The history of the civil law system dates to the sixth century when the Byzantine emperor Justinian codified the laws of Rome.
- Civil *legal systems* should not be confused with the civil (or tort) *laws* found in the United States.
- The civil legal system was established by states or nations for self-regulation; thus, the civil law system can be divided into subdivisions, such as French civil law, German civil law, and so on.
- It is the most widespread legal system in the world and the most common legal system in Europe.
- Under the civil legal system, lower courts are not compelled to follow the decisions made by higher courts.

Common Law System

- Developed in England.
- Based on previous interpretations of laws:
 - In the past, judges would walk throughout the country enforcing laws and settling disputes.

- The judges did not have a written set of laws, so they based their laws on custom and precedent.
- In the 12th century, the king of England (Henry II) imposed a unified legal system that was “common” to the entire country.
- Reflects the community’s morals and expectations.
- Led to the creation of barristers, or lawyers, who actively participate in the litigation process through the presentation of evidence and arguments.
- Today, the common law system uses judges and juries of peers. If the jury trial is waived, the judge decides the facts.
- Typical systems consist of a higher court, several intermediate appellate courts, and many local trial courts. Precedent flows down through this system. Tradition also allows for “magistrate’s courts,” which address administrative decisions.
- The common law system is broken down into criminal, civil/tort, and administrative.

Criminal Law System

- Based on common law, statutory law, or a combination of both.
- Addresses behavior that is considered harmful to society.
- Punishment usually involves a loss of freedom, such as incarceration, or monetary fines.
- Responsibility is on the prosecution to prove guilt beyond a reasonable doubt (innocent until proven guilty).

Civil/Tort Law System

- Offshoot of criminal law.
- Under civil law, the defendant owes a legal duty to the victim. In other words, the defendant is obligated to conform to a particular standard of conduct, usually set by what a “reasonable person of ordinary prudence” would do to prevent foreseeable injury to the victim.
- The defendant’s breach of that duty causes injury to the victim; usually physical or financial.
- Categories of civil law:
 - **Intentional** Examples include assault, intentional infliction of emotional distress, or false imprisonment.
 - **Wrongs against property** An example is nuisance against landowner.
 - **Wrongs against a person** Examples include car accidents, dog bites, and a slip and fall.
 - **Negligence** An example is wrongful death.
 - **Nuisance** An example is trespassing.

- **Dignitary wrongs** Include invasion of privacy and civil rights violations.
- **Economic wrongs** Examples include patent, copyright, and trademark infringement.
- **Strict liability** Examples include a failure to warn of risks and defects in product manufacturing or design.

Administrative (Regulatory) Law System

- Laws and legal principles created by administrative agencies to address a number of areas, including international trade, manufacturing, environment, and immigration.

Customary Law System

- Deals mainly with personal conduct and patterns of behavior.
- Based on traditions and customs of the region.
- Emerged when cooperation of individuals became necessary as communities merged.
- Not many countries work under a purely customary law system, but instead use a mixed system where customary law is an integrated component. (Codified civil law systems emerged from customary law.)
- Mainly used in regions of the world that have mixed legal systems (for example, China and India).
- Restitution is commonly in the form of a monetary fine or service.

Religious Law System

- Based on religious beliefs of the region.
 - In Islamic countries, the law is based on the rules of the Koran.
 - The law, however, is different in every Islamic country.
 - Jurists and clerics have a high degree of authority.
- Covers all aspects of human life, but commonly divided into
 - Responsibilities and obligations to others.
 - Religious duties.
- Knowledge and rules as revealed by God, which define and govern human affairs.
- Rather than create laws, lawmakers and scholars attempt to discover the truth of law.
- Law, in the religious sense, also includes codes of ethics and morality, which are upheld and required by God. For example, Hindu law, Sharia (Islamic law), Halakha (Jewish law), and so on.

Mixed Law System

- Two or more legal systems are used together and apply cumulatively or interactively.

- Most often mixed law systems consist of civil and common law.
- A combination of systems is used as a result of more or less clearly defined fields of application.
- Civil law may apply to certain types of crimes, while religious law may apply to other types within the same region.
- Examples of mixed law systems include those in Holland, Canada, and South Africa.



Common Law Revisited

These different legal systems are certainly complex, and while you are not expected to be a lawyer to pass the CISSP exam, having a high-level understanding of the different types (civil, common, customary, religious, mixed) is important. The exam will dig more into the specifics of the common law legal system and its components. Under the common law legal system, *civil law* deals with wrongs against individuals or organizations that result in damages or loss. This is referred to as *tort law*. Examples include trespassing, battery, negligence, and product liability. A successful civil lawsuit against a defendant would result in financial restitution and/or community service instead of a jail sentence. When someone sues another person in civil court, the jury decides upon *liability* instead of innocence or guilt. If the jury determines the defendant is liable for the act, then the jury decides upon the compensatory and/or punitive damages of the case.

Criminal law is used when an individual's conduct violates the government laws, which have been developed to protect the public. Jail sentences are commonly the punishment for criminal law cases that result in conviction, whereas in civil law cases the punishment is usually an amount of money that the liable individual must pay the victim. For example, in the O.J. Simpson case, the defendant was first tried and found

not guilty in the criminal law case, but then was found liable in the civil law case. This seeming contradiction can happen because the burden of proof is lower in civil cases than in criminal cases.



EXAM TIP Civil law generally is derived from common law (case law), cases are initiated by private parties, and the defendant is found liable or not liable for damages. Criminal law typically is statutory, cases are initiated by government prosecutors, and the defendant is found guilty or not guilty.

Administrative/regulatory law deals with regulatory standards that regulate performance and conduct. Government agencies create these standards, which are usually applied to companies and individuals within those specific industries. Some examples of administrative laws could be that every building used for business must have a fire detection and suppression system, must have clearly visible exit signs, and cannot have blocked doors, in case of a fire. Companies that produce and package food and drug products are regulated by many standards so that the public is protected and aware of their actions. If an administrative law case determines that a company did not abide by specific regulatory standards, officials in the company could even be held accountable. For example, if a company makes tires that shred after a couple of years of use because the company doesn't comply with manufacturing safety standards, the officers in that company could be liable under administrative, civil, or even criminal law if they were aware of the issue but chose to ignore it to keep profits up.

Cybercrimes and Data Breaches

So far, we've discussed laws and regulations only in a general way to provide a bit of context. Let's now dive into the laws and regulations that are most relevant to our roles as cybersecurity leaders. Computer crime laws (sometimes collectively referred to as *cyber-law*) around the world deal with some of the core issues: unauthorized access, modification or destruction of assets, disclosure of sensitive information, and the use of malware (malicious software).

Although we usually only think of the victims and their systems that were attacked during a crime, laws have been created to combat three categories of crimes. A *computer-assisted crime* is where a computer was used as a tool to help carry out a crime. A *computer-targeted crime* concerns incidents where a computer was the victim of an attack crafted to harm it (and its owners) specifically. The last type of crime is where a computer is not necessarily the attacker or the target, but just happened to be involved when a crime was carried out. This category is referred to as *computer is incidental*.

Some examples of computer-assisted crimes are

- Exploiting financial systems to conduct fraud
- Stealing military and intelligence material from government computer systems
- Conducting industrial espionage by attacking competitors and gathering confidential business data

- Carrying out information warfare activities by leveraging compromised influential accounts
- Engaging in hacktivism, which is protesting a government's or organization's activities by attacking its systems and/or defacing its website

Some examples of computer-targeted crimes include

- Distributed denial-of-service (DDoS) attacks
- Stealing passwords or other sensitive data from servers
- Installing cryptominers to mine cryptocurrency on someone else's computers
- Conducting a ransomware attack



NOTE The main issues addressed in computer crime laws are unauthorized modification, disclosure, destruction, or access and inserting malicious programming code.

Some confusion typically exists between the two categories—computer-assisted crimes and computer-targeted crimes—because intuitively it would seem any attack would fall into both of these categories. One system is carrying out the attacking, while the other system is being attacked. The difference is that in computer-assisted crimes, the computer is only being used as a tool to carry out a traditional type of crime. Without computers, people still steal, cause destruction, protest against organizations (for example, companies that carry out experiments upon animals), obtain competitor information, and go to war. So these crimes would take place anyway; the computer is simply one of the tools available to the attacker. As such, it helps that threat actor become more efficient at carrying out a crime.

Computer-assisted crimes are usually covered by regular criminal laws in that they are not always considered a “computer crime.” One way to look at it is that a computer-*targeted* crime could not take place without a computer, whereas a computer-*assisted* crime could. Thus, a computer-targeted crime is one that did not, and could not, exist before use of computers became common. In other words, in the good old days, you could not carry out a buffer overflow on your neighbor or install malware on your enemy's system. These crimes require that computers be involved.

If a crime falls into the “computer is incidental” category, this means a computer just happened to be involved in some secondary manner, but its involvement is still significant. For example, if you have a friend who works for a company that runs the state lottery and he gives you a printout of the next three winning numbers and you type them into your computer, your computer is just the storage place. You could have just kept the piece of paper and not put the data in a computer. Another example is child pornography. The actual crime is obtaining and sharing child pornography pictures or graphics. The pictures could be stored on a file server or they could be kept in a physical file in someone's desk. So if a crime falls within this category, the computer is not attacking another computer and a computer is not being attacked, but the computer is still used in some significant manner.

Because computing devices are everywhere in modern society, computers are incidental to most crimes today. In a fatal car crash, the police may seize the drivers' mobile devices to look for evidence that either driver was texting at the time of the accident. In a domestic assault case, investigators may seek a court order to obtain the contents of the home's virtual assistant, such as Amazon Alexa, because it may contain recorded evidence of the crime.

You may say, "So what? A crime is a crime. Why break it down into these types of categories?" The reason these types of categories are created is to allow current laws to apply to these types of crimes, even though they are in the digital world. Let's say someone is on your computer just looking around, not causing any damage, but she should not be there. Should legislators have to create a new law stating, "Thou shall not browse around in someone else's computer," or should law enforcement and the courts just apply the already created trespassing law? What if a hacker got into a traffic-control system and made all of the traffic lights turn green at the exact same time? Should legislators go through the hassle of creating a new law for this type of activity, or should law enforcement and the courts use the already created (and understood) manslaughter and murder laws? Remember, a crime is a crime, and a computer is just a new tool to carry out traditional criminal activities.

Now, this in no way means countries can just depend upon the laws on the books and that every computer crime can be countered by an existing law. Many countries have had to come up with new laws that deal specifically with different types of computer crimes. For example, the following are just *some* of the laws that have been created or modified in the United States to cover the various types of computer crimes:

- 18 USC 1029: Fraud and Related Activity in Connection with Access Devices
- 18 USC 1030: Fraud and Related Activity in Connection with Computers
- 18 USC 2510 et seq.: Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC 2701 et seq.: Stored Wire and Electronic Communications and Transactional Records Access
- Digital Millennium Copyright Act
- Cyber Security Enhancement Act of 2002



EXAM TIP You do not need to know these laws for the CISSP exam; they are just examples.

Complexities in Cybercrime

Since we have a bunch of laws to get the digital bad guys, this means we have this whole cybercrime thing under control, right? Alas, cybercrimes have only increased over the years and will not stop anytime soon. Several contributing factors explain why these activities have not been properly stopped or even curbed. These include issues related

to proper attribution of the attacks, the necessary level of protection for networks, and successful prosecution once an attacker is captured.

Many attackers are never caught because they spoof their addresses and identities and use methods to cover their digital footsteps. Many attackers break into networks, take whatever resources they were after, and clean the logs that tracked their movements and activities. Because of this, many organizations do not even know their systems have been violated. Even if an attacker's activities are detected, it does not usually lead to the true identity of the individual, though it does alert the organization that a specific vulnerability was exploited.

Attackers commonly hop through several systems before attacking their victim so that tracking down the attackers will be more difficult. This is exemplified by a threat actor approach known as an *island-hopping attack*, which is when the attacker compromises an easier target that is somehow connected to the ultimate one. For instance, consider a major corporation like the one depicted on the right side of Figure 3-1. It has robust cybersecurity and relies on a regional supplier for certain widgets. Since logistics are oftentimes automated, these two companies have trusted channels of communication between them so their computers can talk to each other about when more widgets might be needed and where. The supplier, in turn, relies on a small company that produces special screws for the widgets. This screw manufacturer employs just a couple of people working out of the owner's garage and is a trivial target for an attacker. So, rather than target the major corporation directly, a cybercriminal could attack the screw manufacturer's unsecured computers, use them to gain a foothold in the supplier, and then use that company's trusted relationship with the well-defended target to ultimately get into its systems. This particular type of island-hopping attack is also known as a *supply-chain attack* because it exploits trust mechanisms inherent in supply chains.

Many companies that are victims of an attack usually just want to ensure that the vulnerability the attacker exploited is fixed, instead of spending the time and money to go after and prosecute the attacker. This is a huge contributing factor as to why cybercriminals get away with their activities. Some regulated organizations—for instance, financial institutions—by law, must report breaches. However, most organizations do not have to report breaches or computer crimes. No company wants its dirty laundry out in the open for everyone to see. The customer base will lose confidence, as will

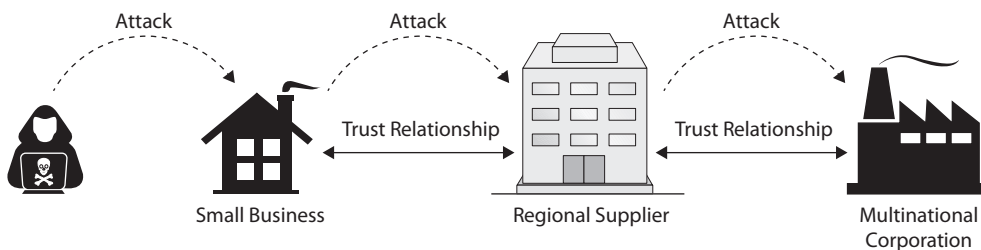


Figure 3-1 A typical island-hopping attack

the shareholders and investors. We do not actually have true computer crime statistics because most are not reported.

Although regulations, laws, and attacks help make senior management more aware of security issues, when their company ends up in the headlines with reports of how they lost control of over 100,000 credit card numbers, security suddenly becomes very important to them.



NOTE Even though some institutions must, by law, report security breaches and crimes, that does not mean they all follow this law. Some of these institutions, just like many other organizations, often simply fix the vulnerability and sweep the details of the attack under the carpet.

The Evolution of Attacks

Perpetrators of cybercrime have evolved from bored teenagers with too much time on their hands to organized crime rings with very defined targets and goals. In the early 1990s, hackers were mainly made up of people who just enjoyed the thrill of hacking. It was seen as a challenging game without any real intent of harm. Hackers used to take down large websites (e.g., Yahoo!, MSN, Excite) so their activities made the headlines and they won bragging rights among their fellow hackers. Back then, virus writers created viruses that simply replicated or carried out some benign activity, instead of the more malicious actions they could have carried out. Unfortunately, today, these trends have taken on more sinister objectives as the Internet has become a place of business. This evolution is what drove the creation of the antivirus (now antimalware) industry.

Three powerful forces converged in the mid to late 1990s to catapult cybercrime forward. First, with the explosive growth in the use of the Internet, computers became much more lucrative targets for criminals. Second, there was an abundance of computer experts who had lost their livelihoods with the end of the Soviet Union. Some of these bright minds turned to cybercrime as a way to survive the tough times in which they found themselves. Finally, with increased demand for computing systems, many software developers were rushing to be first to market, all but ignoring the security (or lack thereof) of their products and creating fertile ground for remote attacks from all over the world. These forces resulted in the emergence of a new breed of cybercriminal possessing knowledge and skills that quickly overwhelmed many defenders. As the impact of the increased threat was realized, organizations around the world started paying more attention to security in a desperate bid to stop their cybercrime losses.

In the early 2000s, there was a shift from cybercriminals working by themselves to the formation of organized cybercrime gangs. This change dramatically improved the capabilities of these threat actors and allowed them to go after targets that, by then, were very well defended. This shift also led to the creation of vast, persistent attack infrastructures on a global scale. After cybercriminals attacked and exploited computers, they maintained a presence for use in support of later attacks. Nowadays, these exploited targets are known as malicious *bots*, and they are usually organized into *botnets*. These botnets can be used to carry out DDoS attacks, transfer spam or pornography, or do whatever the attacker commands the bot software to do. Figure 3-2 shows the many uses cybercriminals have for compromised computers.

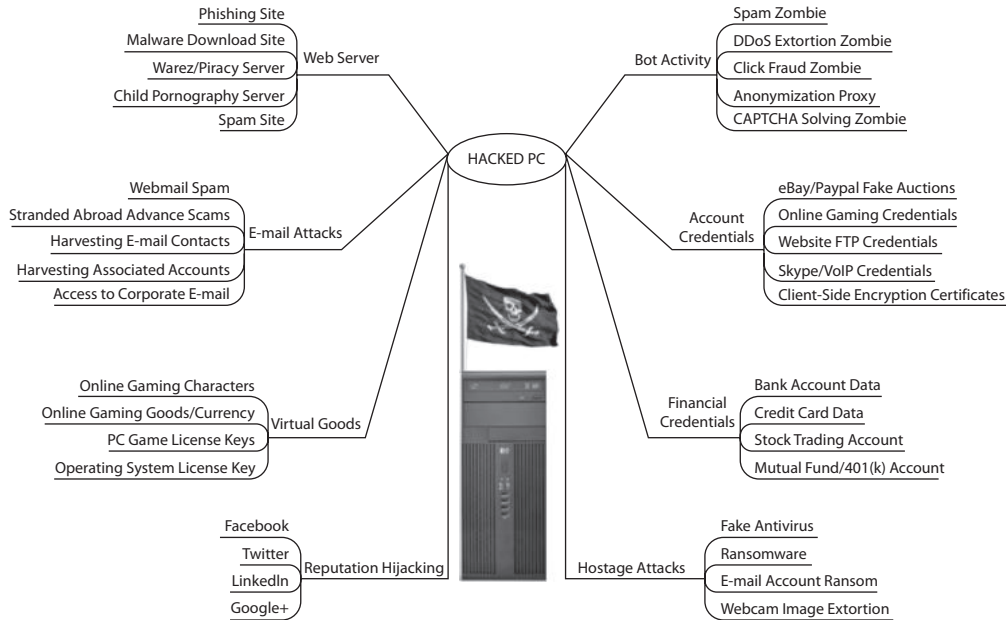


Figure 3-2 Malicious uses for a compromised computer (Source: www.krebsonsecurity.com)



EXAM TIP You may see the term *script kiddies* on the exam (or elsewhere). It refers to hackers who do not have the requisite skills to carry out specific attacks without the tools provided on the Internet or through friends.

A recent development in organized cybercrime is the emergence of so-called Hacking as a Service (HaaS), which is a play on cloud computing services such as Software as a Service (SaaS). HaaS represents the commercialization of hacking skills, providing access to tools, target lists, credentials, hackers for hire, and even customer support. In the last couple of years, there has been a significant increase in the number of marketplaces in which HaaS is available.

Many times hackers are just scanning systems looking for a vulnerable running service or sending out malicious links in e-mails to unsuspecting victims. They are just looking for any way to get into any network. This would be the shotgun approach to network attacks. Another, more dangerous, attacker has you in the proverbial crosshairs and is determined to identify your weakest point and exploit it. As an analogy, the thief that goes around rattling door knobs to find one that is not locked is not half as dangerous as the one who will watch you day in and day out to learn your activity patterns, where you work, what type of car you drive, and who your family is and patiently wait for your most vulnerable moment to ensure a successful and devastating attack.

We call this second type of attacker an *advanced persistent threat (APT)*. This is a military term that has been around for ages, but since the digital world is effectively a

battleground, this term is more relevant each and every day. How an APT differs from the plain old vanilla attacker is that the APT is commonly a group of attackers, not just one hacker, that combine their knowledge and abilities to carry out whatever exploit will get them into the environment they are seeking. The APT is very focused and motivated to aggressively and successfully penetrate a network with various different attack methods and then clandestinely hide its presence while achieving a well-developed, multilevel foothold in the environment.

The “advanced” aspect of the term APT pertains to the expansive knowledge, capabilities, and skill base of the APT. The “persistent” component has to do with the fact that the group of attackers is not in a hurry to launch an attack quickly, but will wait for the most beneficial moment and attack vector to ensure that its activities go unnoticed. This is what we refer to as a “low-and-slow” attack. This type of attack is coordinated by human involvement, rather than just a virus type of threat that goes through automated steps to inject its payload. The APT has specific objectives and goals and is commonly highly organized and well funded, which makes it the biggest threat of all.

APTs commonly use custom-developed malicious code that is built specifically for its target, has multiple ways of hiding itself once it infiltrates the environment, may be able to polymorph itself in replication capabilities, and has several different “anchors” to make it hard to eradicate even if it is discovered. Once the code is installed, it commonly sets up a covert back channel (as regular bots do) so that it can be remotely controlled by the group of attackers. The remote control functionality allows the attackers to traverse the network with the goal of gaining continuous access to critical assets.

APT infiltrations are usually very hard to detect with host-based solutions because the attackers put the code through a barrage of tests against the most up-to-date detection applications on the market. A common way to detect these types of threats is through network traffic changes. For example, changes in DNS queries coming out of your network could indicate that an APT has breached your environment and is using DNS tunneling to establish command and control over the compromised hosts. The APT will likely have multiple control servers and techniques to communicate so that if one connection gets detected and removed, the APT still has an active channel to use. The APT may implement encrypted tunnels over HTTPS so that its data that is in transmission cannot be inspected. Figure 3-3 illustrates the common steps and results of APT activity.

The ways of getting into a network are basically endless (exploit a web service, induce users to open e-mail links and attachments, gain access through remote maintenance accounts, exploit operating systems and application vulnerabilities, compromise connections from home users, etc.). Each of these vulnerabilities has its own fixes (patches, proper configuration, awareness, proper credential practices, encryption, etc.). It is not only these fixes that need to be put in place; we need to move to a more effective situational awareness model. We need to have better capabilities of knowing what is happening throughout our network in near to real time so that our defenses can react quickly and precisely.

The landscape continues to evolve, and the lines between threat actors are sometimes blurry. We already mentioned the difficulty in attributing an attack to a specific individual so that criminal charges may be filed. Something that makes this even harder is the practice among some governments of collaborating with criminal groups in their countries.

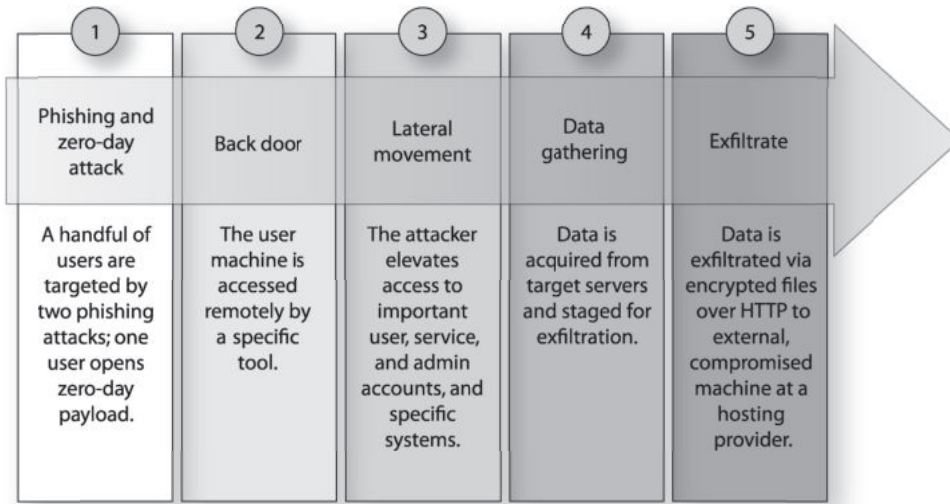


Figure 3-3 Gaining access into an environment and extracting sensitive data

Common Internet Crime Schemes

- Business e-mail compromise
- Business fraud
- Charity and disaster fraud
- Counterfeit prescription drugs
- Credit card fraud
- Election crimes and security
- Identity theft
- Illegal sports betting
- Nigerian letter, or “419”
- Ponzi/pyramid
- Ransomware
- Sextortion

Find out how these types of computer crimes are carried out by visiting <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes>.

Do You Trust Your Neighbor?

Most organizations do not like to think about the fact that the enemy might be inside the organization and working internally. It is more natural to view threats as the faceless unknowns that reside on the outside of our environment. Employees have direct and privileged access to an organization's assets, and they are commonly not as highly monitored compared to traffic that is entering the network from external entities. The combination of too much trust, direct access, and the lack of monitoring allows for a lot of internal fraud and abuse to go unnoticed.

There have been many criminal cases over the years where employees at various organizations have carried out embezzlement or have launched revenge attacks after they were fired or laid off. While it is important to have fortified walls to protect us from the outside forces that want to cause us harm, it is also important to realize that our underbelly is more vulnerable. Employees, contractors, and temporary workers who have direct access to critical resources introduce risks that need to be understood and countermeasured.

The way it works is that the government looks the other way as long as the crimes are committed in other countries. When the government needs a bit of help to obfuscate what it's doing to another government, it enlists the help of the cybercrime gang they've been protecting (or at least tolerating) and tell them what to do and to whom. To the target, it looks like a cybercrime but in reality it had nation-state goals.

So while the sophistication of the attacks continues to increase, so does the danger of these attacks. Isn't that just peachy?

Up until now, we have listed some difficulties of fighting cybercrime: the anonymity the Internet provides the attacker; attackers are organizing and carrying out more sophisticated attacks; the legal system is running to catch up with these types of crimes; and organizations are just now viewing their data as something that must be protected. All these complexities aid the bad guys, but what if we throw in the complexity of attacks taking place between different countries?

International Issues

If a hacker in Ukraine attacks a bank in France, whose legal jurisdiction is that? How do these countries work together to identify the criminal and carry out justice? Which country is required to track down the criminal? And which country should take this person to court? Well, the short answer is: it depends.

When computer crime crosses international boundaries, the complexity of such issues shoots up considerably and the chances of the criminal being brought to any court decreases. This is because different countries have different legal systems, some countries have no laws pertaining to computer crime, jurisdiction disputes may erupt, and some governments may not want to play nice with each other. For example, if someone in Iran attacked a system in Israel, do you think the Iranian government would help Israel track down the attacker? What if someone in North Korea attacked a military system in the

United States? Do you think these two countries would work together to find the hacker? Maybe or maybe not—or perhaps the attack was carried out by a government agency pretending to be a cybercrime gang.

There have been efforts to standardize the different countries' approaches to computer crimes because they happen so easily over international boundaries. Although it is very easy for an attacker in China to send packets through the Internet to a bank in Saudi Arabia, it is very difficult (because of legal systems, cultures, and politics) to motivate these governments to work together.

The *Council of Europe (CoE) Convention on Cybercrime*, also known as the Budapest Convention, is one example of an attempt to create a standard international response to cybercrime. In fact, it is the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation. One of the requirements of the treaty is that signatories develop national legislation outlawing a series of cybercrimes, such as hacking, computer-related fraud, and child pornography. The convention's objectives also include the creation of a framework for establishing jurisdiction and extradition of the accused. For example, extradition can only take place when the event is a crime in both jurisdictions. As of April 2021, 68 countries around the world (not just in Europe) have signed or ratified the treaty, contributing to the global growth in effective cybercrime legislation that is internationally interoperable. According to the United Nations (UN), 79 percent of the world's countries (that's 154) now have cybercrime laws. All these laws vary, of course, but they may impact your own organization depending on where you do business and with whom.

Data Breaches

Among the most common cybercrimes are those relating to the theft of sensitive data. In fact, it is a rare month indeed when one doesn't read or hear about a major data breach. Information is the lifeblood of most major corporations nowadays, and threat actors know this. They have been devoting a lot of effort over the past several years to compromising and exploiting the data stores that, in many ways, are more valuable to organizations than any vault full of cash. This trend continues unabated, which makes data breaches one of the most important issues in cybersecurity today.

In a way, data breaches can be thought of as the opposite of privacy: data owners lose control of who has the ability to access their data. When an organization fails to properly protect the privacy of its customers' data, it increases the likelihood of experiencing a data breach. It should not be surprising, therefore, that some of the same legal and regulatory issues that apply to privacy also apply to data breaches.

It is important to note that data breaches need not involve a violation of personal privacy. Indeed, some of the most publicized data breaches have had nothing to do with personally identifiable information (PII) but with intellectual property (IP). It is worth pausing to properly define the term *data breach* as a security event that results in the actual or potential compromise of the confidentiality or integrity of protected information by unauthorized actors. Protected information can be PII, IP, protected health information (PHI), classified information, or any other information that can cause damage to an individual or organization.

Personally Identifiable Information

Personally identifiable information (PII) is data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. PII needs to be highly protected because it is commonly used in identity theft, financial crimes, and various criminal activities.

While it seems as though defining and identifying PII should be easy and straightforward, what different countries, federal governments, and state governments consider to be PII differs.

The U.S. Office of Management and Budget in its memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." Determining what constitutes PII, then, depends on a specific risk assessment of the likelihood that the information can be used to uniquely identify an individual. This is all good and well, but doesn't really help us recognize information that might be considered PII. Typical components are listed here:

- Full name (if not common)
- National identification number
- Home address
- IP address (in some cases)
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Birthday
- Birthplace
- Genetic information

The following items are less often used because they are commonly shared by so many people, but they can fall into the PII classification and may require protection from improper disclosure:

- First or last name, if common
- Country, state, or city of residence
- Age, especially if nonspecific

- Gender or race
- Name of the school they attend or workplace
- Grades, salary, or job position
- Criminal record

As a security professional, it is important to understand which legal and regulatory requirements are triggered by data breaches. To further complicate matters, most U.S. states, as well as many other countries, have enacted distinct laws with subtle but important differences in notification stipulations. As always when dealing with legal issues, it is best to consult with an attorney. This section is simply an overview of some of the legal requirements of which you should be aware.

U.S. Laws Pertaining to Data Breaches

We've already mentioned various U.S. federal statutes dealing with cybercrimes. Despite our best efforts, there will be times when our information systems are compromised and personal information security controls are breached. Let's briefly highlight some of the laws that are most relevant to data breaches:

- California Consumer Privacy Act (CCPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HI-TECH) Act
- Gramm-Leach-Bliley Act of 1999
- Economic Espionage Act of 1996

It is worth recalling here that data breaches are not only violations of customer privacy. When a threat actor compromises a target corporation's network and exposes its intellectual property, a breach has occurred. While the other laws we have discussed in this section deal with protecting customers' PII, the Economic Espionage Act protects corporations' IP. When you think of data breaches, it is critical that you consider both PII and IP exposure.

Almost every U.S. state has enacted legislation that requires government and private entities to disclose data breaches involving PII. The most important of these is probably the California Consumer Privacy Act, which went into effect in 2020. The CCPA is perhaps the broadest and most far-reaching of U.S. state laws around PII breaches, but it is certainly not the only one. In almost every case, PII is defined by the states as the combination of first and last name with any of the following:

- Social Security number
- Driver's license number
- Credit or debit card number with the security code or PIN

Unfortunately, that is where the commonalities end. The laws are so different that compliance with all of them is a difficult and costly issue for most corporations. In some states, simple access to files containing PII triggers a notification requirement, while in other states the organization must only notify affected parties if the breach is reasonably likely to result in illegal use of the information. Many experts believe that the CCPA will set an example for other states and may provide a template for other countries.

European Union Laws Pertaining to Data Breaches

Global organizations that move data across other country boundaries must be aware of and follow the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Since most countries have a different set of laws pertaining to the definition of private data and how it should be protected, international trade and business get more convoluted and can negatively affect the economy of nations. The OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so that data is properly protected and everyone follows the same type of rules.

The core principles defined by the OECD are as follows:

- **Collection Limitation Principle** Collection of personal data should be limited, obtained by lawful and fair means, and with the knowledge of the subject.
- **Data Quality Principle** Personal data should be kept complete and current and be relevant to the purposes for which it is being used.
- **Purpose Specification Principle** Subjects should be notified of the reason for the collection of their personal information at the time that it is collected, and organizations should only use it for that stated purpose.
- **Use Limitation Principle** Only with the consent of the subject or by the authority of law should personal data be disclosed, made available, or used for purposes other than those previously stated.
- **Security Safeguards Principle** Reasonable safeguards should be put in place to protect personal data against risks such as loss, unauthorized access, modification, and disclosure.
- **Openness Principle** Developments, practices, and policies regarding personal data should be openly communicated. In addition, subjects should be able to easily establish the existence and nature of personal data, its use, and the identity and usual residence of the organization in possession of that data.
- **Individual Participation Principle** Subjects should be able to find out whether an organization has their personal information and what that information is, to correct erroneous data, and to challenge denied requests to do so.
- **Accountability Principle** Organizations should be accountable for complying with measures that support the previous principles.



NOTE Information on the OECD Guidelines can be found at www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

Although the OECD Guidelines were a great start, they were not enforceable or uniformly applied. The European Union in many cases takes individual privacy much more seriously than most other countries in the world, so in 1995 it enacted the Data Protection Directive (DPD). As a directive, it was not directly enforceable, but EU member states were required to enact laws that were consistent with it. The intent of this was to create a set of laws across the EU that controlled the way in which European organizations had to protect the personal data and privacy of EU citizens. The Safe Harbor Privacy Principles were then developed to outline how U.S.-based organizations could comply with European privacy laws. For a variety of reasons, this system of directives, laws, and principles failed to work well in practice and had to be replaced.

The General Data Protection Regulation (GDPR) was adopted by the EU in April 2016 and became enforceable in May 2018. It protects the personal data and privacy of EU citizens. The GDPR, unlike a directive such as the DPD, has the full weight of a law in all 27 member states of the EU. This means that each state does not have to write its own version, which harmonizes data protection regulations and makes it easier for organizations to know exactly what is expected of them throughout the bloc. The catch is that these requirements are quite stringent, and violating them exposes an organization to a maximum fine of 4 percent of that organization's global turnover. For a company like Google, that would equate to over \$4 billion if they were ever shown to not be in compliance. Ouch!

The GDPR defines three relevant entities:

- **Data subject** The individual to whom the data pertains
- **Data controller** Any organization that collects data on EU residents
- **Data processor** Any organization that processes data for a data controller

The regulation applies if any one of the three entities is based in the EU, but it also applies if a data controller or processor has data pertaining to an EU resident. The GDPR impacts every organization that holds or uses European personal data both inside and outside of Europe. In other words, if your organization is a U.S.-based company that has never done business with the EU, but it has an EU citizen working as a summer intern, it probably has to comply with the GDPR or risk facing stiff penalties.

The GDPR set of protected types of privacy data is more inclusive than regulations and laws outside the EU. Among others, protected privacy data includes

- Name
- Address
- ID numbers

- Web data (location, IP address, cookies)
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

To ensure this data is protected, the GDPR requires that most data controllers and data processors formally designate a Data Protection Officer (DPO). DPOs are internal compliance officers that act semi-independently to ensure that their organizations follow the letter of the regulation. While DPOs are not ultimately responsible if their organizations are not in compliance (at least according to the GDPR), in practice they are charged with monitoring compliance, advising controllers on when and how to conduct data protection impact assessments, and maintaining all required records.

Key provisions of the GDPR include

- **Consent** Data controllers and data processors cannot use personal data without explicit consent of the data subjects.
- **Right to be informed** Data controllers and data processors must inform data subjects about how their data is, will, or could be used.
- **Right to restrict processing** Data subjects can agree to have their data stored by a collector but disallow it to be processed.
- **Right to be forgotten** Data subjects can request that their personal data be permanently deleted.
- **Data breaches** Data controllers must report a data breach to the supervisory authority of the EU member state involved within 72 hours of becoming aware of it.

Other Nations' Laws Pertaining to Data Breaches

As might be expected, the rest of the world is a hodgepodge of laws with varying data breach notification conditions and requirements. As of this writing, the United Nations lists at least 62 countries that have no legally mandated notification requirements whatsoever. This is concerning because unscrupulous organizations have been known to outsource their data-handling operations to countries with no data breach laws in order to circumvent the difficulties in reconciling the different country and state requirements.

The EU's GDPR, though it has been called too restrictive and costly by some, has served as a model for other countries to implement similar legislation. For example, the two newest data protection laws, which came into full effect in 2020, are Brazil's General Personal Data Protection Law (Lei Geral de Proteção de Dados, or LGPD) and Thailand's Personal Data Protection Act (PDPA). Both apply to all organizations that handle the personal information of these countries' residents, whether they are physically located within the country or not. Thailand's PDPA further provides for jail time in particularly egregious cases.

Again, you do not need to know all these international laws to become a CISSP. However, you need to be aware that they exist and may impact your business and cybersecurity even if you didn't know your organization had interests in those countries. It is best to consult your organization's legal or compliance team to determine which laws apply to your own team.

Import/Export Controls

Another complexity that comes into play when an organization is attempting to work with organizations in other parts of the world is import and export laws. Each country has its own specifications when it comes to what is allowed in its borders and what is allowed out. For example, the *Wassenaar Arrangement* implements export controls for "Conventional Arms and Dual-Use Goods and Technologies." It is currently made up of 42 countries and lays out rules on how the following items can be exported from country to country:

- **Category 1** Special Materials and Related Equipment
- **Category 2** Material Processing
- **Category 3** Electronics
- **Category 4** Computers
- **Category 5** Part 1: Telecommunications
- **Category 5** Part 2: Information Security
- **Category 6** Sensors and Lasers
- **Category 7** Navigation and Avionics
- **Category 8** Marine
- **Category 9** Aerospace and Propulsion

The main goal of the Wassenaar Arrangement is to prevent the buildup of military capabilities that could threaten regional and international security and stability. So, everyone is keeping an eye on each other to make sure no one country's weapons can take everyone else out. The idea is to try and make sure everyone has similar offensive and defensive military capabilities with the hope that we won't end up blowing each other up.

One item the agreement deals with is cryptography, which is considered a *dual-use good* because it can be used for both military and civilian purposes. The agreement recognizes the danger of exporting products with cryptographic functionality to countries that are in the "offensive" column, meaning that they are thought to have friendly ties with terrorist organizations and/or want to take over the world through the use of weapons of mass destruction. If the "good" countries allow the "bad" countries to use cryptography, then the "good" countries cannot snoop and keep tabs on what the "bad" countries are up to.

The specifications of the Wassenaar Arrangement are complex and always changing. Which countries fall within the "good" and "bad" categories changes, and what can be exported to whom and how changes. In some cases, no products that contain

cryptographic functions can be exported to a specific country; some countries are allowed to import only products with limited cryptographic functions; some countries require certain licenses to be granted; and other countries (the “good” countries) have no restrictions.

While the Wassenaar Arrangement deals mainly with the exportation of items, some countries (China, Russia, Iran, etc.) have cryptographic *import* restrictions that have to be understood and followed. These countries do not allow their citizens to use cryptography because they believe that the ability to monitor many aspects of a citizen’s online activities is essential to effectively governing people. This obviously gets very complex for companies who sell products that use integrated cryptographic functionality. One version of the product may be sold to China if it has no cryptographic functionality. Another version may be sold to Russia if a certain international license is in place. A fully functioning product can be sold to Canada, because who are they ever going to hurt?

It is important to understand the import and export requirements your organization must meet when interacting with entities in other parts of the world. You could inadvertently break a country’s law or an international treaty if you do not get the right type of lawyers involved in the beginning and follow the approved processes.

Transborder Data Flow

While import and export controls apply to products, a much more common asset that constantly moves in and out of every country is data, and, as you might imagine at this point, there are laws, regulations, and processes that address what data can be moved where, when, why, how, and by whom. A *transborder data flow (TDF)* is the movement of machine-readable data across a political boundary such a country’s border. This data is generated or acquired in one country but may be stored and processed in other countries as a result of TDFs. In a modern, connected world, this happens all the time. For example, just imagine all the places your personal data will go when you make an airline reservation to travel overseas, especially if you have a layover along the way.



NOTE Transborder data flows are sometimes called cross-border data flows.

Some governments control transborder data flows by enacting *data localization* laws that require certain types of data to be stored and processed within the borders of their respective country, sometimes exclusively. There are many reasons for these laws, but they pretty much boil down to protecting their citizens, either by ensuring a higher standard of privacy protection or by allowing easier monitoring of their actions (typically the things citizens try to do overseas). Data localization can increase the cost of doing business in some countries because your organization may have to provision (and protect) information systems in that country that it otherwise wouldn’t.

Ironically, the very technology trend that initially fueled data localization concerns, cloud computing services, ultimately became an important tool to address those concerns

in a cost-effective manner. At their onset, cloud computing services promised affordable access to resources around the globe, sometimes by shifting loads and storage from one region to another. In recent years, the major cloud service providers have adapted to localization laws by offering an increasing number of regions (sometimes down to individual countries) where the data is guaranteed to remain.

Privacy

Privacy is becoming more threatened as the world increasingly relies on computing technology. There are several approaches to addressing privacy, including the generic approach and regulation by industry. The generic approach is *horizontal enactment*—rules that stretch across all industry boundaries. It affects all industries, including government. Regulation by industry is *vertical enactment*. It defines requirements for specific verticals, such as the financial sector and health care. In both cases, the overall objective is twofold. First, the initiatives seek to protect citizens' personally identifiable information. Second, the initiatives seek to balance the needs of government and businesses to collect and use PII with consideration of security issues.

In response, countries have enacted privacy laws. For example, although the United States already had the Federal Privacy Act of 1974, it has enacted new laws, such as the Gramm-Leach-Bliley Act of 1999 and HIPAA, in response to an increased need to protect personal privacy information. These are examples of a vertical approach to addressing privacy, whereas the EU's GDPR, Canada's Personal Information Protection and Electronic Documents Act, and New Zealand's Privacy Act of 1993 are horizontal approaches. Most countries nowadays have some sort of privacy requirements in their laws and regulations, so we need to be aware of their impact on our information systems and their security to avoid nasty legal surprises.

Licensing and Intellectual Property Requirements

Another way to get into trouble, whether domestically or internationally, is to run afoul of intellectual property laws. As previously introduced, *intellectual property (IP)* is a type of property created by human intellect. It consists of ideas, inventions, and expressions that are uniquely created by a person and can be protected from unauthorized use by others. Examples are song lyrics, inventions, logos, and secret recipes. IP laws do not necessarily look at who is right or wrong, but rather how an organization or individual can protect what it rightfully owns from unauthorized duplication or use and what it can do if these laws are violated.

So who designates what constitutes authorized use? The owner of the IP does this by granting licenses. A *license* is an agreement between an IP owner (the licensor) and somebody else (the licensee), granting that party the right to use the IP in very specific ways. For example, the licensee can only use the IP for a year unless they renew the license (presumably after paying a subscription fee). A license can also be, and frequently is, nontransferable, meaning only the licensees, and not their family members or friends, can use it. Another common provision in the agreement is whether or not the license will be exclusive to the licensee.

Licenses can become moot if the IP is not properly protected by the licensor. An organization must implement safeguards to protect resources that it claims to be intellectual property and must show that it exercised due care (reasonable acts of protection) in its efforts to protect those resources. For example, if an employee sends a file to a friend and the company terminates the employee based on the activity of illegally sharing IP, then in a wrongful termination case brought by the employee, the company must show the court why this file is so important to the company, what type of damage could be or has been caused as a result of the file being shared, and, most important, what the company had done to protect that file. If the company did not secure the file and tell its employees that they were not allowed to copy and share that file, then the company will most likely lose the case. However, if the company implemented safeguards to protect that file and had an acceptable use policy in its employee manual that explained that copying and sharing the information within the file was prohibited and that the punishment for doing so could be termination, then the company could not be found liable of wrongfully terminating the employee.

Intellectual property can be protected by different legal mechanisms, depending upon the type of resource it is. As a CISSP, you should be knowledgeable of four types of IP laws: trade secrets, copyrights, trademarks, and patents. These topics are addressed in depth in the following sections, followed by tips on protecting IP internally and combating software piracy.

Trade Secret

Trade secret law protects certain types of information or resources from unauthorized use or disclosure. For a company to have its resource qualify as a trade secret, the resource must provide the company with some type of competitive value or advantage. A trade secret can be protected by law if developing it requires special skill, ingenuity, and/or expenditure of money and effort. This means that a company cannot say the sky is blue and call it a trade secret.

A *trade secret* is something that is proprietary to a company and important for its survival and profitability. An example of a trade secret is the formula used for a soft drink, such as Coke or Pepsi. The resource that is claimed to be a trade secret must be confidential and protected with certain security precautions and actions. A trade secret could also be a new form of mathematics, the source code of a program, a method of making the perfect jelly bean, or ingredients for a special secret sauce. A trade secret has no expiration date unless the information is no longer secret or no longer provides economic benefit to the company.

Many companies require their employees to sign a nondisclosure agreement (NDA), confirming that they understand its contents and promise not to share the company's trade secrets with competitors or any unauthorized individuals. Companies require an NDA both to inform the employees of the importance of keeping certain information secret and to deter them from sharing this information. Having employees sign the NDA also gives the company the right to fire an employee or bring charges if the employee discloses a trade secret.

A low-level engineer working at Intel took trade secret information that was valued by Intel at \$1 billion when he left his position at the company and went to work at his new employer, rival chipmaker Advanced Micro Devices (AMD). Intel discovered that this person still had access to Intel's most confidential information even after starting work at AMD. He even used the laptop that Intel provided to him to download 13 critical documents that contained extensive information about the company's new processor developments and product releases. Unfortunately, these stories are not rare, and companies are constantly dealing with challenges of protecting the very data that keeps them in business.

Copyright

In the United States, *copyright law* protects the right of the creator of an original work to control the public distribution, reproduction, display, and adaptation of that original work. The law covers many categories of work: pictorial, graphic, musical, dramatic, literary, pantomime, motion picture, sculptural, sound recording, and architectural. Copyright law does not cover the specific resource, as does trade secret law. It protects the *expression* of the idea of the resource instead of the resource itself. A copyright is usually used to protect an author's writings, an artist's drawings, a programmer's source code, or specific rhythms and structures of a musician's creation. Computer programs and manuals are just two examples of items protected under the Federal Copyright Act. The program or manual is covered under copyright law once it has been written. Although including a warning and the copyright symbol (©) is not required, doing so is encouraged so others cannot claim innocence after copying another's work.

Copyright protection does not extend to any method of operations, process, concept, or procedure, but it does protect against unauthorized copying and distribution of a protected work. It protects the form of expression rather than the subject matter. A patent deals more with the subject matter of an invention; copyright deals with how that invention is represented. In that respect, copyright is weaker than patent protection, but the duration of copyright protection is longer. Copyright protection exists for the life of the creator plus 70 years. If the work was created jointly by multiple authors, the 70 years start counting after the death of the last surviving one.

Computer programs can be protected under the copyright law as literary works. The law protects both the source code and object code, which can be an operating system, application, or database. In some instances, the law can protect not only the code but also the structure, sequence, and organization. The user interface is part of the definition of a software application structure; therefore, one vendor cannot copy the exact composition of another vendor's user interface.

Copyright infringement cases have exploded in numbers since the rise of "warez" sites that use the common BitTorrent protocol. BitTorrent is a peer-to-peer file sharing protocol and is one of the most common protocols for transferring large files. Warez is a term that refers to copyrighted works distributed or traded without fees or royalties, in general violation of the copyright law. The term generally refers to unauthorized releases by groups, as opposed to file sharing between friends.

Once a warez site posts copyrighted material, it is very difficult to have it removed because law enforcement is commonly overwhelmed with larger criminal cases and does not have the bandwidth to go after these “small fish.” Another issue with warez sites is that the actual servers may reside in another country; thus, legal jurisdiction makes things more difficult and the country that the server resides within may not even have a copyright law. Film and music recording companies have had the most success in going after these types of offenders because they have the funds and vested interest to do so.

Trademark

A *trademark* is slightly different from a copyright in that it is used to protect a word, name, symbol, sound, shape, color, or combination of these. The reason a company would trademark one of these, or a combination, is that it represents the company (brand identity) to a group of people or to the world. Companies have marketing departments that work very hard to create something new that will cause the company to be noticed and stand out in a crowd of competitors, and trademarking the result of this work with a government registrar is a way of properly protecting it and ensuring others cannot copy and use it.

Companies cannot trademark a number or common word. This is why companies create new names—for example, Intel’s Pentium and Apple’s iPhone. However, unique colors can be trademarked, as well as identifiable packaging, which is referred to as “trade dress.” Thus, Novell Red and UPS Brown are trademarked, as are some candy wrappers.

Registered trademarks are generally protected for ten years, but can be renewed for another ten years indefinitely. In the United States, you must file paperwork with the U.S. Patent and Trademark Office (USPTO) between the fifth and sixth years showing that you are actually using the trademark. This means that you can’t just create a trademark you don’t ever use and still keep others from using it. You have to file another “Declaration of Use” between the ninth and tenth year, and then every nine to ten years thereafter.



NOTE In 1883, international harmonization of trademark laws began with the Paris Convention, which in turn prompted the Madrid Agreement of 1891. Today, international trademark law efforts and international registration are overseen by the World Intellectual Property Organization (WIPO), an agency of the United Nations. The United States is a party to this agreement.

There have been many interesting trademark legal battles over the years. In one case a person named Paul Specht started a company named “Android Data” and had his company’s trademark approved in 2002. Specht’s company failed, and although he attempted to sell it and the trademark, he had no buyers. When Google announced that it was going to release a new mobile operating system called Android, Specht built a new website using his old company’s name to try and prove that he was indeed still using this trademark. Specht took Google to court and asked for \$94 million in trademark infringement damages. The court ruled in Google’s favor and found that Google was not liable for damages.

Patent

Patents are given to individuals or organizations to grant them legal ownership of, and enable them to exclude others from using or copying, the invention covered by the patent. The invention must be novel, useful, and not obvious—which means, for example, that a company could not patent air. Thank goodness. If a company figured out how to patent air, we would have to pay for each and every breath we took!

After the inventor completes an application for a patent and it is approved, the patent grants a limited property right to exclude others from making, using, or selling the invention for a specific period of time. For example, when a pharmaceutical company develops a specific drug and acquires a patent for it, that company is the only one that can manufacture and sell this drug until the stated year in which the patent is up (usually 20 years from the date of approval). After that, the information is in the public domain, enabling all companies to manufacture and sell this product, which is why the price of a drug drops substantially after its patent expires and generic versions hit the market.

The patent process also applies to algorithms. If an inventor of an algorithm acquires a patent, she has full control over who can use the algorithm in their products. If the inventor lets a vendor incorporate the algorithm, she will most likely get a fee and possibly a license fee on each instance of the product that is sold.

Patents are ways of providing economic incentives to individuals and organizations to continue research and development efforts that will most likely benefit society in some fashion. Patent infringement is huge within the technology world today. Large and small product vendors seem to be suing each other constantly with claims of patent infringement. The problem is that many patents are written at a very high level. For example, if Inge developed a technology that accomplishes functionality A, B, and C, you could actually develop your own technology in your own way that also accomplished A, B, and C. You might not even know that Inge's method or patent existed; you just developed this solution on your own. Yet if Inge did this type of work first and obtained the patent, then she could go after you legally for infringement.



EXAM TIP A patent is the strongest form of intellectual property protection.

The amount of patent litigation in the technology world is remarkable. In October 2020, Centripetal Networks won a \$1.9 billion award against Cisco Systems involving network threat detection technologies. In April of the same year, Apple and Broadcom were ordered to pay Caltech \$1.1 billion because they infringed multiple Caltech patents pertaining to wireless error correction codes. Even though the amounts of these awards are certainly eye-popping, they are not the only notable ones. It turns out that 2020 was a pretty rough year for Apple, because it was also ordered to pay \$506 million to PanOptis and another \$109 million to WiLAN in two other infringement cases.

This is just a brief list of recent patent litigation. These patent cases are like watching 100 Ping-Pong matches going on all at the same time, each containing its own characters and dramas, and involving millions and billions of dollars.



Figure 3-4 Defendants added to litigation campaigns by year (Data provided by RPX Corporation on 12/14/20. © 2020 RPX Corporation)

While the various vendors are fighting for market share in their respective industries, another reason for the increase in patent litigation is the emergence of nonpracticing entities (NPEs), also known as patent trolls. NPE (or patent troll) is a term used to describe a person or company who obtains patents, not to protect their invention, but to aggressively and opportunistically go after another entity that tries to create something based upon them. A patent troll has no intention of manufacturing an item based upon their patent, but wants to get licensing fees from an entity that does manufacture the item. For example, let's say that Donald has ten new ideas for ten different technologies. He puts them through the patent process and gets them approved, but he has no intention of putting in all the money and risk it takes to actually create these technologies and attempt to bring them to market. He is going to wait until you do this and then he is going to sue you for infringing upon his patent. If he wins the court case, you have to pay him licensing fees for the product you developed and brought to market.

It is important to do a patent search before putting effort into developing a new methodology, technology, or business method. As you can see in Figure 3-4, there is a lot of litigation due to patent infringement, and thousands of new defendants are being added to the party each year. These cases are very costly but can oftentimes be avoided with a bit of homework.

Internal Protection of Intellectual Property

Ensuring that specific resources are protected by the previously mentioned laws is very important, but other measures must be taken internally to make sure the resources that are confidential in nature are properly identified and protected.

The resources protected by one of the previously mentioned laws need to be identified and integrated into the organization's data classification scheme. This should be directed by management and carried out by the IT staff. The identified resources should have the necessary level of access control protection, auditing enabled, and a proper

storage environment. If a resource is deemed secret, then not everyone in the organization should be able to access it. Once the individuals who are allowed to have access are identified, their level of access and interaction with the resource should be defined in a granular method. Attempts to access and manipulate the resource should be properly audited, and the resource should be stored on a protected system with the necessary security mechanisms.

Employees must be informed of the level of secrecy or confidentiality of the resource and of their expected behavior pertaining to that resource.

If an organization fails in one or all of these steps, it may not be covered by the laws described previously, because it may have failed to practice due care and properly protect the resource that it has claimed to be so important to the survival and competitiveness of the organization.

Software Piracy

Software piracy occurs when the intellectual or creative work of an author is used or duplicated without permission or compensation to the author. It is an act of infringement on ownership rights, and if the pirate is caught, he could be sued civilly for damages, be criminally prosecuted, or both.

When a vendor develops an application, it usually licenses the program rather than sells it outright. The license agreement contains provisions relating to the approved use of the software and the corresponding manuals. If an individual or organization fails to observe and abide by those requirements, the license may be terminated and, depending on the actions, criminal charges may be leveled. The risk to the vendor that develops and licenses the software is the loss of profits it would have earned.

There are four categories of software licensing. *Freeware* is software that is publicly available free of charge and can be used, copied, studied, modified, and redistributed without restriction. *Shareware*, or *trialware*, is used by vendors to market their software. Users obtain a free, trial version of the software. Once the user tries out the program, the user is asked to purchase a copy of it. *Commercial* software is, quite simply, software that is sold for or serves commercial purposes. And, finally, *academic* software is software that is provided for academic purposes at a reduced cost. It can be open source, freeware, or commercial software.

Some software vendors sell bulk licenses, which enable several users to use the product simultaneously. These master agreements define proper use of the software along with restrictions, such as whether corporate software can also be used by employees on their home machines. One other prevalent form of software licensing is the End User License Agreement (EULA). It specifies more granular conditions and restrictions than a master agreement. Other vendors incorporate third-party license-metering software that keeps track of software usability to ensure that the customer stays within the license limit and otherwise complies with the software licensing agreement.

The information security officer should be aware of all these types of contractual commitments required by software companies. This person needs to be educated on the restrictions the organization is under and make sure proper enforcement mechanisms are in place. If an organization is found guilty of illegally copying software or using

more copies than its license permits, the security officer in charge of this task may be primarily responsible.

Thanks to easy access to high-speed Internet, employees' ability—if not the temptation—to download and use pirated software has greatly increased. The June 2018 BSA Global Software Survey, a study conducted by the Business Software Alliance (BSA) and International Data Corporation (IDC), found that 37 percent of the software installed on personal computers globally was not properly licensed. This means that for every two dollars' worth of legal software that is purchased, one dollar's worth is pirated. Software developers often use these numbers to calculate losses resulting from pirated copies. The assumption is that if the pirated copy had not been available, then everyone who is using a pirated copy would have instead purchased it legally.

Not every country recognizes software piracy as a crime, but several international organizations have made strides in curbing the practice. The Federation Against Software Theft (FAST) and the Business Software Alliance (author of the Global Software Survey) are organizations that promote the enforcement of proprietary rights of software. This is a huge issue for companies that develop and produce software, because a majority of their revenue comes from licensing fees. The study also estimates that the total economic damage experienced by the industry was \$46.3 billion in losses in 2018.

One of the offenses an individual or organization can commit is to decompile vendor object code. This is usually done to figure out how the application works by obtaining the original source code, which is confidential, and perhaps to reverse-engineer it in the hope of understanding the intricate details of its functionality. Another purpose of reverse-engineering products is to detect security flaws within the code that can later be exploited. This is how some buffer overflow vulnerabilities are discovered.

Many times, an individual decompiles the object code into source code and either finds security holes to exploit or alters the source code to produce some type of functionality that the original vendor did not intend. In one example, an individual decompiled a program that protects and displays e-books and publications. The vendor did not want anyone to be able to copy the e-publications its product displayed and thus inserted an encoder within the object code of its product that enforced this limitation. The individual decompiled the object code and figured out how to create a decoder that would overcome this restriction and enable users to make copies of the e-publications, which infringed upon those authors' and publishers' copyrights.

The individual was arrested and prosecuted under the *Digital Millennium Copyright Act (DMCA)*, which makes it illegal to create products that circumvent copyright protection mechanisms. Interestingly enough, many computer-oriented individuals protested this person's arrest, and the company prosecuting (Adobe) quickly decided to drop all charges.

DMCA is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures that are put into place to protect copyright material. So if you figure out a way to "unlock" the proprietary way that Barnes & Noble protects its e-books, you can be charged under this act. Even if you don't share the actual copyright-protected books with someone, you still broke this specific law and can be found guilty.



NOTE The European Union passed a similar law called the Copyright Directive.

Compliance Requirements

While it is important to know *which* specific laws and regulations your organization needs to be compliant with, it is also important to know *how* to ensure that compliance is being met and how to properly convey that to the necessary stakeholders. If it hasn't already done so, your organization should develop a compliance program that outlines what needs to be put into place to be compliant with the necessary internal and external drivers. Then, an audit team should periodically assess how well the organization is doing to meet the identified requirements.

The first step is to identify which laws and regulations your organization needs to be compliant with (e.g., GDPR, HIPAA, PCI DSS, etc.). This will give you the specific requirements that the laws and regulations impose on your organization. The requirements, in turn, inform your risk assessment and allow you to select the appropriate controls to ensure compliance. Once this is all done and tested, the auditors have stuff to audit. These auditors can be internal or external to the organization and will have long checklists of items that correspond with the legal, regulatory, and policy requirements the organization must meet.



NOTE Audits and auditors will be covered in detail in Chapter 18.

It is common for organizations to develop *governance, risk, and compliance (GRC)* programs, which allow for the integration and alignment of the activities that take place in each one of these silos of a security program. If the same *key performance indicators (KPIs)* are used in the governance, risk, and compliance auditing activities, then the resulting reports can effectively illustrate the overlap and integration of these different concepts. For example, if a healthcare organization is not compliant with various HIPAA requirements, this is a type of risk that management must be aware of so that it can ensure the right activities and controls are put into place. Also, how does executive management carry out security governance if it does not understand the risks the organization is facing and the outstanding compliance issues? It is important for all of these things to be understood by the decision makers in a holistic manner so that they can make the best decisions pertaining to protecting the organization as a whole. The agreed-upon KPI values are commonly provided to executive management in dashboards or scorecard formats, which allow management to quickly understand the health of the organization from a GRC point of view.

Contractual, Legal, Industry Standards, and Regulatory Requirements

Regulations in computer and information security cover many areas for many different reasons. We've already covered some of these areas, such as data privacy, computer misuse, software copyright, data protection, and controls on cryptography. These regulations can be implemented in various arenas, such as government and private sectors, for reasons dealing with environmental protection, intellectual property, national security, personal privacy, public order, health and safety, and prevention of fraudulent activities.

Security professionals have so much to keep up with these days, from understanding how the latest ransomware attacks work and how to properly protect against them, to inventorying sensitive data and ensuring it only exists in approved places with the right protections. Professionals also need to follow which new security products are released and how they compare to the existing products. This is followed up by keeping track of new technologies, service patches, hotfixes, encryption methods, access control mechanisms, telecommunications security issues, social engineering, and physical security. Laws and regulations have been ascending the list of things that security professionals also need to be aware of. This is because organizations must be compliant with more and more laws and regulations, both domestically and internationally, and noncompliance can result in a fine or a company going out of business, and in some cases certain executive management individuals ending up in jail.

Laws, regulations, and directives developed by governments or appointed agencies do not usually provide detailed instructions to follow to properly protect computers and company assets. Each environment is too diverse in topology, technology, infrastructure, requirements, functionality, and personnel. Because technology changes at such a fast pace, these laws and regulations could never successfully represent reality if they were too detailed. Instead, they state high-level requirements that commonly puzzle organizations about how to be compliant with them. This is where the security professional comes to the rescue.

In the past, security professionals were expected to know how to carry out penetration tests, configure firewalls, and deal only with the technology issues of security. Today, security professionals are being pulled out of the server rooms and asked to be more involved in business-oriented issues. As a security professional, you need to understand the laws and regulations that your organization must comply with and what controls must be put in place to accomplish compliance. This means the security professional now must have a foot in both the technical world and the business world.

But it's not just laws and regulations you need to be aware of. Your organization may also need to be compliant with certain standards in order to be competitive (or even do business) in certain sectors. If your organization processes credit cards, then it has to comply with the Payment Card Industry Data Security Standard (PCI DSS). This is not a law or even a government regulation; instead, it is an example of a mandatory industry standard. If your organization is a financial institution that is considered part of the critical national infrastructure of the United Kingdom, then it may have to comply with the CBEST standard even though any reputable organization in that

sector is expected to do so voluntarily. And, finally, if your organization wants to sell cloud services to the U.S. government, it won't even be considered unless it is Federal Risk and Authorization Management Program (FedRAMP) certified. So, compliance is not just about laws and regulations. There are many other standards that may be critical to the success of your organization.

Another compliance requirement that is sometimes missed by cybersecurity professionals is related to contracts and other legally binding agreements. In the course of doing business, your organization may enter into agreements that may have security requirements. For example, your organization may partner with another organization and thereby gain access to its sensitive data. The partnering agreement may have a clause requiring both organizations to ensure that they have certain controls in place to protect that data. If these protections are not already part of your own security architecture and you fail to implement them (or even become aware of them), you would not be in compliance with the contractual obligations, which could make your organization liable in the event of a breach. The point is that we need to have open lines of communication with our legal and business colleagues to ensure we are made aware of any security clauses before we enter into a contract.

If You Are Not a Lawyer, You Are Not a Lawyer

Many times organizations ask their security professionals to help them figure out how to be compliant with the necessary laws and regulations. While you might be aware of and have experience with some of these laws and regulations, there is a high likelihood that you are not aware of all the necessary federal and state laws, regulations, and international requirements your organization must meet. These laws, regulations, and directives morph over time and new ones are added, and while you may think you are interpreting them correctly, you may be wrong. It is critical that an organization get its legal department involved with compliancy issues. Many security professionals have been in this situation over many years. At many organizations, the legal staff does not know enough about all of these issues to ensure the organization is properly protected. In this situation, advise the organization to contact outside counsel to help them with these issues.

Organizations look to security professionals to have all the answers, especially in consulting situations. You will be brought in as the expert. But if you are not a lawyer, you are not a lawyer and should advise your customer properly in obtaining legal help to ensure proper compliance in all matters. The increasing use of cloud computing is adding an incredible amount of legal and regulatory compliance confusion to current situations.

It is a good idea to have a clause in any type of consulting agreement you use that explicitly outlines these issues so that if and when the organization gets hauled to court after a computer breach, your involvement will be understood and previously documented.

Over time, the CISSP exam has become more global in nature and less U.S.-centric. Specific questions on U.S. laws and regulations have been taken out of the test, so you do not need to spend a lot of time learning them and their specifics. Be familiar with why laws are developed and put in place and their overall goals, instead of memorizing specific laws and dates.

Privacy Requirements

Privacy compliance requirements stem from the various data protection laws and regulations we've already covered in this chapter (for example, CCPA, GDPR, and HIPAA). The hard part is ensuring you are aware of all the localities within which your organization gathers, stores, and processes various types of private data. The good news is that, at their core, these laws are not all that different from one another in terms of the security controls they require. In almost every case, the controls are reasonable things we would want to have anyway. So, most of the work you'll require to remain compliant is pretty straightforward.

Where things get a bit murkier is when we consider what data is covered and when we are required to notify someone. For example, the GDPR covers PII on EU persons and HIPAA covers PHI on any patient treated by a U.S. healthcare provider. So, if you suffer a data breach affecting the PHI of a German national who received care in your U.S. facilities, you will most likely have to follow both reporting procedures in these two laws. Under the GDPR, you'd have 72 hours from the time of discovery, while under HIPAA, you could have up to 60 days. The notified parties, in addition to the individual whose information was compromised, vary in each case, which further complicates things.

The best approach is collaborate with your business and legal colleague to develop detailed notification procedures that cover each potential breach. Once you're satisfied that your organization can comply with the notification requirements, you should exercise different scenarios to test the procedures and ensure everyone is trained on how to execute them. A breach will ruin your day all by itself, so there's no sense in adding the need to figure out compliance requirements at the point of crisis to make it worse. Furthermore, having procedures that are periodically exercised can help prove to any investigators that you were doing the right things all along.

Liability and Its Ramifications

Executives may be held responsible and liable under various laws and regulations. They could be sued by stockholders and customers if they do not practice due diligence and due care. *Due diligence* can be defined as doing everything within one's power to prevent a bad thing from happening. Examples of this would be setting appropriate policies, researching the threats and incorporating them into a risk management plan, and ensuring audits happen at the right times. *Due care*, on the other hand, means taking the precautions that a reasonable and competent person would take in the same situation. For example, someone who ignores a security warning and clicks through to a malicious website would fail to exercise due care.



EXAM TIP Due diligence is normally associated with leaders, laws, and regulations. Due care is normally applicable to everyone, and failure to exercise it could be used to show negligence.

Before you can figure out how to properly protect yourself, you need to find out what it is you are protecting yourself against. This is what due diligence is all about—researching and assessing the current level of vulnerabilities so the true risk level is understood. Only after these steps and assessments take place can effective controls and safeguards be identified and implemented.

Due Care vs. Due Diligence

Due diligence is the act of gathering the necessary information so the best decision-making activities can take place. Before a company purchases another company, it should carry out due diligence activities so that the purchasing company does not have any “surprises” down the road. The purchasing company should investigate all relevant aspects of the past, present, and predictable future of the business of the target company. If this does not take place and the purchase of the new company hurts the original company financially or legally, the decision makers could be found liable (responsible) and negligent by the shareholders.

In information security, similar data gathering should take place so that there are no “surprises” down the road and the risks are fully understood before they are accepted. If a financial company is going to provide online banking functionality to its customers, the company needs to fully understand all the risks this service entails for the company. Website hacking attempts will increase, account fraud attempts will increase, database attacks will increase, social engineering attacks will increase, and so forth. While this company is offering its customers a new service, it is also making itself a juicier target for attackers and lawyers. The company needs to carry out due diligence to understand all these risks before offering this new service so that the company can make the best business decisions. If it doesn’t implement proper countermeasures, the company opens itself up to potential criminal charges, civil suits, regulatory fines, loss of market share, and more.

Due care pertains to acting responsibly and “doing the right thing.” It is a legal term that defines the standards of performance that can be expected, either by contract or by implication, in the execution of a particular task. Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

If an organization does not have sufficient security policies, necessary countermeasures, and proper security awareness training in place, it is not practicing due care and can be found negligent. If a financial institution that offers online banking does not implement TLS for account transactions, for example, it is not practicing due care.

Many times due diligence (data gathering) has to be performed so that proper due care (prudent actions) can take place.