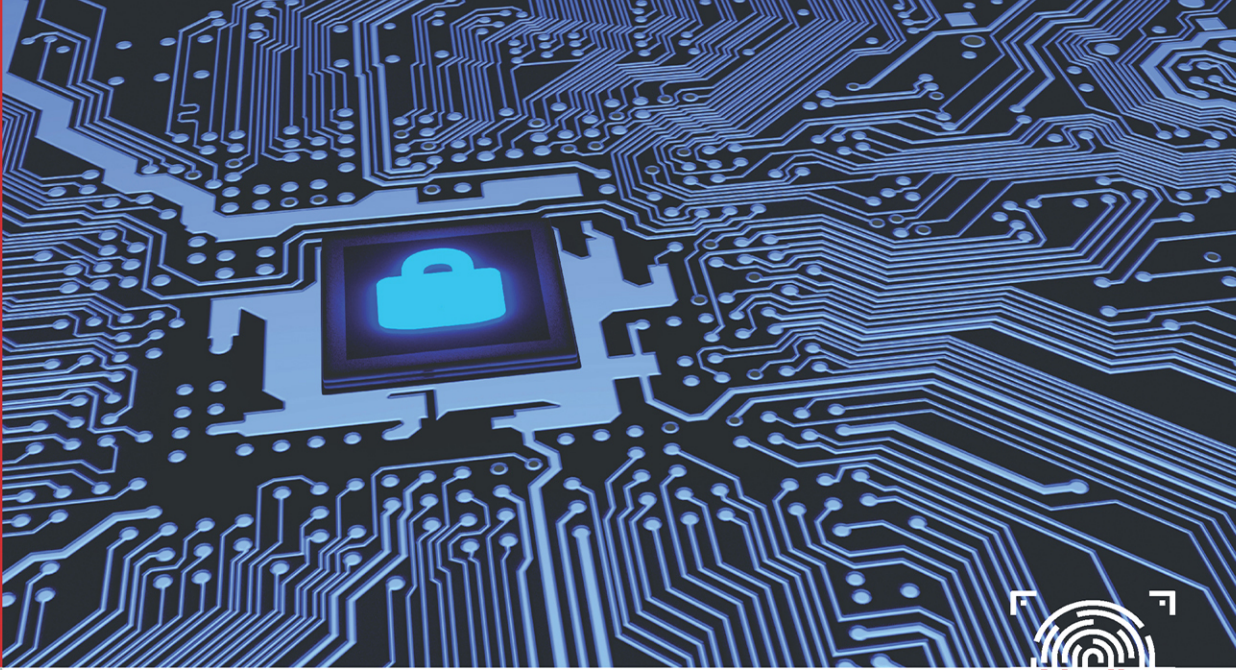
PEARSON IT CYBERSECURITY CURRICULUM



DEVELOPING CYBERSECURITY PROGRAMS AND POLICIES

OMAR SANTOS

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Developing Cybersecurity Programs and Policies

Omar Santos

Pearson

Developing Cybersecurity Programs and Policies

Copyright © 2019 by Pearson Education, Inc.

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

ISBN-13: 978-0-7897-5940-5

ISBN-10: 0-7897-5940-3

Library of Congress Control Number: 2018942730

01 18

Trademarks

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

Warning and Disclaimer

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

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Executive Editor
Mary Beth Ray

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Barbara Hacha

Indexer
Erika Millen

Proofreader
Larry Sulky

Technical Editors
Sari Greene
Klee Michaelis

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
codemantra

Contents at a Glance

1 Understanding Cybersecurity Policy and Governance 2

2 Cybersecurity Policy Organization, Format, and Styles 38

3 Cybersecurity Framework. 72

4 Governance and Risk Management 104

5 Asset Management and Data Loss Prevention. 144

6 Human Resources Security 178

7 Physical and Environmental Security. 208

8 Communications and Operations Security 236

9 Access Control Management. 294

10 Information Systems Acquisition, Development, and Maintenance 338

11 Cybersecurity Incident Response 368

12 Business Continuity Management 426

13 Regulatory Compliance for Financial Institutions 462

14 Regulatory Compliance for the Health-Care Sector. 502

15 PCI Compliance for Merchants 546

16 NIST Cybersecurity Framework 582

Appendix A: Cybersecurity Program Resources 608

Appendix B: Answers to the Multiple Choice Questions 618

Index. 624

Table of Contents

Chapter 1: Understanding Cybersecurity Policy and Governance 2

Information Security vs. Cybersecurity Policies 4

Looking at Policy Through the Ages 5

Policy in Ancient Times. 5

The United States Constitution as a Policy Revolution 6

Policy Today. 6

Cybersecurity Policy 9

What Are Assets? 9

Successful Policy Characteristics 11

What Is the Role of Government? 17

Additional Federal Banking Regulations 21

Government Cybersecurity Regulations in Other Countries 21

The Challenges of Global Policies 22

Cybersecurity Policy Life Cycle 22

Policy Development 23

Policy Publication 24

Policy Adoption 26

Policy Review. 26

Summary 27

Chapter 2: Cybersecurity Policy Organization, Format, and Styles 38

Policy Hierarchy. 39

Standards. 39

Baselines 40

Guidelines 42

Procedures. 42

Plans and Programs 43

Writing Style and Technique 44

Using Plain Language 44

The Plain Language Movement 45

Plain Language Techniques for Policy Writing 46

Policy Format 49

Understand Your Audience 49

Policy Format Types 49

Policy Components 51

Summary 62

Chapter 3: Cybersecurity Framework 72

Confidentiality, Integrity, and Availability 73

What Is Confidentiality? 74

What Is Integrity? 77

What Is Availability? 78

Who Is Responsible for CIA? 82

NIST's Cybersecurity Framework 83

What Is NIST's Function? 83

So, What About ISO? 84

NIST Cybersecurity Framework 85

ISO Standards 86

Summary 93

Chapter 4: Governance and Risk Management 104

Understanding Cybersecurity Policies 105

What Is Governance? 105

What Is Meant by Strategic Alignment? 105

Regulatory Requirements 107

User-Level Cybersecurity Policies 108

Vendor Cybersecurity Policies 108
Cybersecurity Vulnerability Disclosure Policies 108
Client Synopsis of Cybersecurity Policies. 108
Who Authorizes Cybersecurity Policy? 110
What Is a Distributed Governance Model? 111
Evaluating Cybersecurity Policies 114
Revising Cybersecurity Policies: Change Drivers. 117
NIST Cybersecurity Framework Governance Subcategories and Informative References 118
Regulatory Requirements 120
Cybersecurity Risk 122
Is Risk Bad?. 123
Understanding Risk Management 123
Risk Appetite and Tolerance. 126
What Is a Risk Assessment? 127
Risk Assessment Methodologies. 129
Summary 132

Chapter 5: Asset Management and Data Loss Prevention 144

Information Assets and Systems 145
Who Is Responsible for Information Assets? 146
Information Classification 148
How Does the Federal Government Classify Data?. 150
Why Is National Security Information Classified Differently?. 152
Who Decides How National Security Data Is Classified? 153
How Does the Private Sector Classify Data? 154
Can Information Be Reclassified or Even Declassified? 156
Labeling and Handling Standards 156
Why Label? 156
Why Handling Standards? 157

Information Systems Inventory. 159

Why an Inventory Is Necessary and What Should Be Inventoried. 159

Understanding Data Loss Prevention Technologies. 164

Summary 167

Chapter 6: Human Resources Security 178

The Employee Life Cycle 179

What Does Recruitment Have to Do with Security?. 181

What Happens in the Onboarding Phase? 187

What Is User Provisioning? 187

What Should an Employee Learn During Orientation?. 188

Why Is Termination Considered the Most Dangerous Phase? 189

The Importance of Employee Agreements 191

What Are Confidentiality or Nondisclosure Agreements? 191

What Is an Acceptable Use Agreement?. 191

The Importance of Security Education and Training 193

Influencing Behavior with Security Awareness 194

Teaching a Skill with Security Training. 194

Security Education Is Knowledge Driven 194

Summary 196

Chapter 7: Physical and Environmental Security 208

Understanding the Secure Facility Layered Defense Model 210

How Do We Secure the Site?. 211

How Is Physical Access Controlled?. 213

Protecting Equipment 217

No Power, No Processing?. 217

How Dangerous Is Fire? 219

What About Disposal? 221
Stop, Thief!. 224
Summary 226

Chapter 8: Communications and Operations Security 236

Standard Operating Procedures 238
Why Document SOPs? 238
Developing SOPs 239
Operational Change Control. 243
Why Manage Change? 243
Why Is Patching Handled Differently? 248
Malware Protection 250
Are There Different Types of Malware? 251
How Is Malware Controlled? 253
What Is Antivirus Software? 254
Data Replication 258
Is There a Recommended Backup or Replication Strategy?. 259
Secure Messaging. 261
What Makes Email a Security Risk? 262
Are Email Servers at Risk? 265
Other Collaboration and Communication Tools 266
Activity Monitoring and Log Analysis. 267
What Is Log Management? 268
Service Provider Oversight 274
What Is Due Diligence?. 274
What Should Be Included in Service Provider Contracts? 275
Threat Intelligence and Information Sharing 278
How Good Is Cyber Threat Intelligence if It Cannot Be Shared? 279
Summary 281

Chapter 9: Access Control Management 294

Access Control Fundamentals 295

What Is a Security Posture? 296

How Is Identity Verified? 298

What Is Authorization? 303

Accounting 306

Infrastructure Access Controls 307

Why Segment a Network? 308

What Is Layered Border Security? 311

Remote Access Security 317

User Access Controls 321

Why Manage User Access? 322

What Types of Access Should Be Monitored? 325

Summary 327

Chapter 10: Information Systems Acquisition, Development, and Maintenance 338

System Security Requirements 339

What Is SDLC? 339

What About Commercially Available or Open Source Software? 342

The Testing Environment 344

Protecting Test Data 344

Secure Code 345

The Open Web Application Security Project (OWASP) 346

Cryptography 350

Why Encrypt? 351

Regulatory Requirements 352

What Is a “Key”? 352

What Is PKI? 353

Why Protect Cryptographic Keys? 354

Digital Certificate Compromise 355

Summary 357

Chapter 11: Cybersecurity Incident Response 368

Incident Response. 369

What Is an Incident? 370

How Are Incidents Reported? 376

What Is an Incident Response Program? 379

The Incident Response Process 381

Tabletop Exercises and Playbooks 383

Information Sharing and Coordination. 384

Computer Security Incident Response Teams 385

Product Security Incident Response Teams (PSIRTs) 387

Incident Response Training and Exercises 396

What Happened? Investigation and Evidence Handling 397

Documenting Incidents. 398

Working with Law Enforcement 398

Understanding Forensic Analysis. 399

Data Breach Notification Requirements 402

Is There a Federal Breach Notification Law? 403

Does Notification Work? 408

Summary 411

Chapter 12: Business Continuity Management 426

Emergency Preparedness. 427

What Is a Resilient Organization? 428

Regulatory Requirements 429

Business Continuity Risk Management. 430

What Is a Business Continuity Threat Assessment? 430

What Is a Business Continuity Risk Assessment? 432

What Is a Business Impact Assessment? 433

The Business Continuity Plan. 436

Roles and Responsibilities 437

Disaster Response Plans 440

Operational Contingency Plans 444

The Disaster Recovery Phase 445

The Resumption Phase. 448

Plan Testing and Maintenance 449

Why Is Testing Important? 449

Plan Maintenance 450

Summary 453

Chapter 13: Regulatory Compliance for Financial Institutions 462

The Gramm-Leach-Bliley Act 463

What Is a Financial Institution? 463

Regulatory Oversight 465

What Are the Interagency Guidelines? 468

New York's Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500) 480

What Is a Regulatory Examination? 482

Examination Process. 483

Examination Ratings 483

Personal and Corporate Identity Theft. 484

What Is Required by the Interagency Guidelines Supplement A? 484

What Is Required by the Supplement to the Authentication in an Internet Banking Environment Guidance? 486

Summary 488

Chapter 14: Regulatory Compliance for the Health-Care Sector 502

The HIPAA Security Rule 504

What Is the Objective of the HIPAA Security Rule? 505

How Is the HIPAA Security Rule Organized? 506

What Are the Physical Safeguards?. 517

What Are the Technical Safeguards?. 520

What Are the Organizational Requirements? 524

What Are the Policies and Procedures Standards? 525

The HIPAA Security Rule Mapping to NIST Cybersecurity Framework 526

The HITECH Act and the Omnibus Rule 527

What Changed for Business Associates? 528

What Are the Breach Notification Requirements? 530

Understanding the HIPAA Compliance Enforcement Process 532

Summary 534

Chapter 15: PCI Compliance for Merchants 546

Protecting Cardholder Data 547

What Is the PAN? 548

The Luhn Algorithm. 549

What Is the PCI DDS Framework?. 550

Business-as-Usual Approach. 551

What Are the PCI Requirements? 552

PCI Compliance. 563

Who Is Required to Comply with PCI DSS? 563

What Is a Data Security Compliance Assessment? 564

What Is the PCI DSS Self-Assessment Questionnaire (SAQ)? 566

Are There Penalties for Noncompliance? 567

Summary 569

Chapter 16: NIST Cybersecurity Framework 582

Introducing the NIST Cybersecurity Framework Components 583

The Framework Core 585

Identify 587

Protect 588

Detect. 589

Respond. 590

Recover 590

Framework Implementation Tiers (“Tiers”) 591

Who Should Coordinate the Framework Implementation? 594

NIST’s Recommended Steps to Establish or Improve a Cybersecurity Program 595

Communication with Stakeholders and Supply Chain Relationships 595

NIST’s Cybersecurity Framework Reference Tool 597

Adopting the NIST Cybersecurity Framework in Real Life. 599

Summary 601

Appendix A: Cybersecurity Program Resources 608

Appendix B: Answers to the Multiple Choice Questions 618

Index 624

About the Author

Omar Santos is a principal engineer in the Cisco Product Security Incident Response Team (PSIRT) within the Cisco Security Research and Operations. He mentors and leads engineers and incident managers during the investigation and resolution of security vulnerabilities in all Cisco products, including cloud services. Omar has been working with information technology and cybersecurity since the mid-1990s. Omar has designed, implemented, and supported numerous secure networks for Fortune 100 and 500 companies and the U.S. government. Prior to his current role, he was a technical leader within the World-Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations.

Omar is an active member of the security community, where he leads several industrywide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar often delivers technical presentations at many conferences and to Cisco customers and partners. He is the author of dozens of books and video courses. You can follow Omar on any of the following:

Personal website: omarsantos.io

Twitter: @santosomar

LinkedIn: https://www.linkedin.com/in/santosomar

Dedication

I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

I also dedicate this book to my father, Jose, and to the memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

Acknowledgments

This manuscript is a result of concerted efforts of various individuals—without their help, this book would have not been a reality. I would like to thank the technical reviewers Sari Green and Klee Michaelis for their significant contributions and expert guidance.

I would also like to express my gratitude to Chris Cleveland, development editor, and Mary Beth Ray, executive editor, for their help and continuous support during the development of this book.

We Want to Hear from You!

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

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

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

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

Email: feedback@pearsonitcertification.com

Introduction

The number of cyber attacks continues to rise. Demand for safe and secure data and other concerns mean that companies need professionals to keep their information safe. Cybersecurity risk includes not only the risk of a data breach, but also the risk of the entire organization being undermined via business activities that rely on digitization and accessibility. As a result, learning how to develop an adequate cybersecurity program is crucial for any organization. Cybersecurity can no longer be something that you delegate to the information technology (IT) team. Everyone needs to be involved, including the Board of Directors.

This book focuses on industry-leading practices and standards, such as the International Organization for Standardization (ISO) standards and the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Special Publications. This book provides detailed guidance on how to effectively develop a cybersecurity program within your organization. This book is intended for anyone who is preparing for a leadership position in business, government, academia, financial services, or health-care. Mastering the material presented in this book is a must for any cybersecurity professional.

This book starts by providing an overview of cybersecurity policy and governance, and how to create cybersecurity policies and develop a cybersecurity framework. It then provides details about governance, risk management, asset management, and data loss prevention. You will learn how to incorporate human resource, physical, and environmental security as important elements of your cybersecurity program. This book also teaches you best practices in communications and operations security, access control management, and information systems acquisition, development, and maintenance. You will learn principles of cybersecurity incident response and how to develop an incident response plan. Organizations across the globe have to be aware of new cybersecurity regulations and how they affect their business in order to remain compliant. Compliance is especially crucial because the punishments for noncompliance typically include large fines. Three chapters in this book cover regulatory compliance for financial institutions and health-care institutions and provide detailed insights about the Payment Card Industry Data Security Standard (PCI DSS). The last chapter provides an overview of the NIST Cybersecurity Framework, and Appendix A provides comprehensive lists of resources covered throughout the book. Anyone—from cybersecurity engineers to incident managers, auditors, and executives—can benefit from the material covered in this book.

This page intentionally left blank

Chapter 7

Physical and Environmental Security

Chapter Objectives

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

- Define the concept of physical security and how it relates to information security.
- Evaluate the security requirements of facilities, offices, and equipment.
- Understand the environmental risks posed to physical structures, areas within those structures, and equipment.
- Enumerate the vulnerabilities related to reusing and disposing of equipment.
- Recognize the risks posed by the loss or theft of mobile devices and media.
- Develop policies designed to ensure the physical and environmental security of information, information systems, and information-processing and storage facilities.

In the beginning of the computer age, it was easy to protect the systems; they were locked away in a lab, weighed thousands of pounds, and only a select few were granted access. Today, computing devices are ubiquitous. We are tasked with protecting devices that range from massive cloud-based multiplex systems to tiny handheld devices. The explosion of both distributed and mobile computing means that computing devices can be located anywhere in the world and are subject to local law and custom. Possession requires that each individual user take responsibility for mobile device security.

Security professionals are often so focused on technical controls that they overlook the importance of physical controls. The simple reality is that physical access is the most direct path to malicious activity, including unauthorized access, theft, damage, and destruction. Protection mechanisms include controlling the physical security perimeter and physical entry, creating secure offices, rooms, and facilities, and implementing barriers to access, such as monitoring, and alerting. Section 11 of ISO 27002:2013 encompasses both physical and environmental security. Environmental security refers to the workplace environment, which includes the design and construction of the facilities, how and where people move, where equipment is stored, how the equipment is secured, and protection from natural and man-made disasters.

In previous chapters, you learned that to properly protect organizational information, we must first know where it is and how critical it is to the organization. Just as we shouldn’t spend as much money or resources to protect noncritical information as we would to protect critical information, so it goes that we shouldn’t spend the same amount to protect a broom closet as we should to protect information-processing facilities such as data centers, server rooms, or even offices containing client information.

Information security professionals rarely have the expertise to address this security domain on their own. It is critical to involve facilities and physical security personnel in strategic and tactical decisions, policies, and procedures. For example, the information security expert designs a server room with a double steel door, card-reading lock, and a camera outside the door. A facilities expert may question the construction of the walls, floor, vents, and ceilings, the capability of the HVAC and fire suppression systems, as well as the potential for a natural disaster, such as an earthquake, fire, or flood. A physical security expert may question the location, the topography, and even the traffic patterns of pedestrians, automobiles, and airplanes. Creating and maintaining physical and environmental security is a team effort.

In this chapter, we focus on design, obstacles, monitoring, and response as they relate to secure areas, equipment security, and environmental controls. We examine the security issues, related best practices, and of course, physical and environmental security policies.

FYI: ISO/IEC 27002:2013 and NIST Cybersecurity Framework

Section 11 of ISO 27002:2013 is dedicated to physical and environmental security, with the objective of maintaining a secure physical environment to prevent unauthorized access, damage, and interference to business premises. Special attention is paid to disposal and destruction.

The NIST Cybersecurity Framework addresses physical security in three areas:

- Under the Protect Identity Management, Authentication and Access Control (PR.AC) Category stating that physical access to assets must be managed and protected
- Under the Information Protection Processes and Procedures (PR.IP) Category stating that policy and regulations regarding the physical operating environment for organizational assets must be met
- Under the Security Continuous Monitoring (DE.CM) Category stating that the physical environment needs to be monitored to detect potential cybersecurity events

Corresponding NIST guidance is provided in the following documents:

- **SP 800-12:** “An Introduction to Computer Security—The NIST Handbook”
- **SP 800-14:** “Generally Accepted Principles and Practices for Securing Information Technology Systems”

- **SP 800-88:** “Guidelines for Media Sanitization”
- **SP 800-100:** “Information Security Handbook: A Guide for Managers”
- **SP 800-116 Rev. 1:** “A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)”
- **SP 800-116:** “A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)”
- **SP 800-183:** “Networks of ‘Things’”

Understanding the Secure Facility Layered Defense Model

The premise of a ***layered defense model*** is that if an intruder can bypass one layer of controls, the next layer of controls should provide additional deterrence or detection capabilities. Layered defense is both physical and psychological. The mere fact that an area *appears* to be secure is in itself a deterrent. Imagine the design of a medieval castle. The castle itself was built of stone. It was sited high on a hill within a walled property. There may have been a moat and an entry drawbridge. There were certainly lookouts and guards. For intruders to launch a successful attack, they had to overcome and penetrate each of these obstacles. The same concept is used in designing secure buildings and areas.

FYI: How Can You Ensure Physical Security of Assets When Your Data and Applications are in the Cloud?

Mature cloud providers such as Amazon Web Services (AWS) provide detailed explanations of their physical and operational security processes for the network and server infrastructure. These are the servers that will host your applications and data in the cloud that you do not have any control over. AWS details all their physical security practices at the following white paper:

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

The white paper details:

“AWS’s data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely."

The paper describes their methodologies and capabilities for the following:

- Fire detection and suppression systems to reduce risk of fire.
- Data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. This includes the use of uninterruptible power supply (UPS) units to provide back-up power and the use of generators.
- Climate and temperature control required to maintain a constant operating temperature for servers and other hardware.
- Management and monitoring of electrical, mechanical, and life support systems and equipment so that any issues are immediately identified.
- Storage device decommissioning when a storage device has reached the end of its useful life, to prevent customer data from being exposed to unauthorized individuals. AWS states that it follows the NIST SP 800-88 ("Guidelines for Media Sanitization") as part of their decommissioning process.

How Do We Secure the Site?

Depending on the size of the organization, information-processing facilities can range from a closet with one server to an entire complex of buildings with several thousand or even hundreds of thousands of computers. In addressing site physical security, we need to think of the most obvious risks, such as theft and other malicious activity, but we also must consider accidental damage and destruction related to natural disasters.

Location

The design of a secure site starts with the location. Location-based threats that need to be evaluated include political stability, susceptibility to terrorism, the crime rate, adjacent buildings, roadways, flight paths, utility stability, and vulnerability to natural disasters. Historical and predictive data can be used to establish both criminal and natural disaster chronology for a geographic area. The outcome will influence the type of security measures that an organization should implement. Best practices dictate that critical information-processing facilities be inconspicuous and unremarkable. They should not have signage relating to their purpose, nor should their outward appearance hint at what may be inside.

FYI: Crime Prevention Through Environmental Design (CPTED)

CPTED (pronounced *sep-ted*) has as its basic premise that the proper design and effective use of the physical environment can lead to a reduction in the incidence and fear of crime. CPTED is a psychological and sociological method of looking at security based upon three constructs:

- People protect territory they feel is their own, and people have a certain respect for the territory of others.
- Intruders do not want to be seen.
- Limiting access discourages intruders and/or marks them as intruders.

The International CPTED Association (ICA) is committed to creating safer environments and improving the quality of life through the use of CPTED principles and strategies. You can learn more about this design concept at www.cpted.net.

Perimeter Security

The three elements to security are obstacles that deter trivial attackers and delay serious ones, detection systems that make it more likely that the attack will be noticed, and a response capability to repel or catch attackers. Obstacles include physical elements such as berms, fences, gates, and bollards. Lighting is also a valuable deterrent. Entrances, exits, pathways, and parking lots should be illuminated. Fences should be at least eight feet in height, with a two-foot parameter of light used to illuminate along the top portion of the fence. The candlepower of the lighting must meet security standards. Detection systems include IP cameras, closed-circuit TV, alarms, motion sensors, and security guards. Response systems include locking gates and doors, on-site or remote security personnel notification, and direct communication with local, county, or state police.

In Practice

Physical Security Perimeter Policy

Synopsis: Securing the perimeter is the first line of defense against external physical attacks. Perimeter controls are required to prevent unauthorized access and damage to facilities.

Policy Statement:

- The company will establish physical security perimeters around business premises.
- An annual risk assessment of all existing business premises and information-processing facilities will be performed to determine the type and strength of the security perimeter that is appropriate and prudent.
- A risk assessment must be conducted on all new sites under consideration prior to building plans being finalized.

- The Office of Facilities Management in conjunction with the Office of Information Security will conduct the risk assessment.
- Risk assessment results and recommendations are to be submitted to the Chief Operating Officer (COO).
- The Office of Facilities Management is responsible for the implementation and maintenance of all physical security perimeter controls.

How Is Physical Access Controlled?

Our next area to consider is physical entry and exit controls. What does it take to get in and out? How is trouble detected and reported? Depending on the site and level of security required, a plethora of access controls are available, including cameras, security guards, mantraps, locks, barriers, metal detectors, biometric scanners, fire-resistant exterior walls that are solid and heavy, and unbreakable/shatterproof glass. The biggest challenge is authorized entry.

Authorizing Entry

How does a company identify authorized personnel, such as employees, contractors, vendors, and visitors? Of greatest concern are the fraudulent or forged credentials obtained through careful profiling or the carelessness of authenticated employees. One commonly used option is a badging system. Badges may also function as access cards. Visitors to secure areas should be credentialed and authorized. Tailgating is one of the most common physical security challenges of all time. In some cases, it might be done innocently by an authorized individual opening a door and holding it open for others, visitors without badges, or someone who looks to be an employee. A number of visitor management systems facilitate ID scanning and verification, photo storage, credentialing, check in and check out, notifications, and monitoring. Visitors should be required to wear some kind of identification that can be evaluated from a distance. For instance, we might choose to have three different colored badges for visitors, which tell our employees what level of supervision should be expected, even if they view the person from across a 100-foot room. If a blue badge denotes close supervision, and you see someone wearing a blue badge without any supervision, you would know immediately to report the visitor or perhaps activate a silent alarm without having to confront or even come within close proximity of the individual. You can install the most advanced security system in the industry, but your security measures will fail if your employees are not educated about the associated security risks. You need to create a secure building culture and good security awareness campaigns.

Background Checks

Your organization should also establish formal policies and procedures to delineate the minimum standards for logical and physical access to your premises and infrastructure hosts. Typically, enterprise organizations conduct criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and matching with the employee’s position within the company and required level of access. The policies also identify functional responsibilities for the administration of physical access during working hours and after hours (including weekends and holidays).

In Practice

Physical Entry Controls Policy

Synopsis: Authorization and identification are required for entry to all nonpublic company locations.

Policy Statement:

- Access to all nonpublic company locations will be restricted to authorized persons only.
- The Office of Human Resources is responsible for providing access credentials to employees and contractors.
- The Office of Facilities Management is responsible for visitor identification, providing access credentials, and monitoring access. All visitor management activities will be documented.
- Employees and contractors are required to visibly display identification in all company locations.
- Visitors are required to display identification in all nonpublic company locations.
- Visitors are to be escorted at all times.
- All personnel must be trained to immediately report unescorted visitors.

Securing Offices, Rooms, and Facilities

In addition to securing building access, the organization needs to secure the workspaces within the building. Workspaces should be classified based on the level of protection required. The classification system should address personnel security, information systems security, and document security. The security controls must take into consideration workplace violence, intentional crime, and environmental hazards.

Secure design controls for spaces within a building include (but are not limited to) the following:

- Structural protection, such as full-height walls, fireproof ceilings, and restricted vent access
- Alarmed solid, fireproof, lockable, and observable doors
- Alarmed locking, unbreakable windows
- Monitored and recorded entry controls (keypad, biometric, card swipe)
- Monitored and recorded activity

In Practice

Workspace Classification

Synopsis: A classification system will be used to categorize workspaces. Classifications will be used to design and communicate baseline security controls.

Policy Statement:

- The company will use a four-tiered workspace classification schema consisting of secure, restricted, nonpublic, and public.
- The company will publish definitions for each classification.
- The criteria for each level will be maintained by and available from the Office of Facilities Management.
- All locations will be associated with one of the four data classifications. Classification assignment is the joint responsibility of the Office of Facilities Management and the Office of Information Security.
- Each classification must have documented security requirements.
- The COO must authorize exceptions.

Working in Secure Areas

It is not enough to just physically secure an area. Close attention must be paid to who is allowed to access the area and what they are allowed to do. Access control lists should be reviewed frequently. If the area is continually monitored, there should be guidelines specifying what is considered "suspicious" activity. If the area is videoed and not continually monitored, then there should be documented procedures regarding how often and by whom the video should be reviewed. Depending on the circumstances, it may be prudent to restrict cameras or recording devices, including smartphones, tablets, and USB drives, from being taken into the area.

In Practice

Working in Secure Areas Policy

Synopsis: Areas classified as "secure" will be continually monitored. Use of recording devices will be forbidden.

Policy Statement:

- All access to areas classified as "secure" will be continually monitored.
- All work in areas classified as "secure" will be recorded. The recordings will be maintained for a period of 36 months.
- Mobile data storage devices are prohibited and may not be allowed in areas classified as "secure" without the authorization of the system owner or Information Security Officer (ISO).
- Audio- and video-recording equipment is prohibited and may not be allowed in areas classified as "secure" without the authorization of the system owner or the Office of Information Security.
- This policy is in addition to workspace classification security protocols.

Ensuring Clear Desks and Clear Screens

Documents containing protected and confidential information are subject to intentional or accidental unauthorized disclosure unless secured from viewing by unauthorized personnel when not in use. The same holds true for computer screens. Companies have a responsibility to protect physical and digital information both during the workday and during nonbusiness hours. All too often, organizations make it *easy* for unauthorized users to view information. Unauthorized access can be the result of viewing a document left unattended or in plain sight, removing (or reprinting) a document from a printer, copier, or fax machine, stealing digital media, such as a DVD or USB drive, and even ***shoulder surfing***, which is the act of looking over someone's shoulder to see what is displayed on a monitor or device.

Protected or confidential documents should never be viewable by unauthorized personnel. When not in use, documents should be locked in file rooms, cabinets, or desk drawers. Copiers, scanners, and fax machines should be located in nonpublic areas and require use codes. Printers should be assigned to users with similar access rights and permissions and located close to the designated users. Users should be trained to retrieve printed documents immediately. Monitors and device screens should be situated to ensure privacy. Password-protected screen savers should be set to engage automatically. Users should be trained to lock their screens when leaving devices unattended. Physical security expectations and requirements should be included in organizational acceptable use agreements.

In Practice

Clear Desk and Clear Screen Policy

Synopsis: User controls are required to prevent the unauthorized viewing or taking of information.

Policy Statement:

- When left unattended during business hours, desks shall be clear of all documents classified as "protected" or "confidential."
- During nonbusiness hours, all documents classified as "protected" or "confidential" will be stored in a secure location.
- While in use, device displays of any type must be situated to not allow unauthorized viewing.
- When left unattended during business hours, device displays should be cleared and locked to prevent viewing.
- Protected and confidential documents should be printed only to assigned printers. Print jobs should be retrieved immediately.
- Scanners, copiers, and fax machines must be locked when not in use and require user codes to operate.

Protecting Equipment

Now that we have defined how facilities and work areas will be secured, we must address the security of the equipment within these facilities. Traditionally, protection controls were limited to company-owned equipment. This is no longer the case. Increasingly, organizations are encouraging employees and contractors to “bring your own device” to work (referred to as BYOD). These devices may store, process, or transmit company information. In developing policies, we need to consider how best to protect both company- and employee-owned equipment from unauthorized access, theft, damage, and destruction.

No Power, No Processing?

No power, no processing—it’s that simple. Long before computers took over the business world, organizations have been taking steps to ensure that power is available. Of course, it is now more important than ever. All information systems rely on clean, consistent, and abundant supplies of electrical power. Even portable devices that run on battery power require electricity for replenishment. Power is not free. Quite the contrary: Power can be very expensive, and excessive use has an environmental and geopolitical impact.

Power Protection

To function properly, our systems need consistent power delivered at the correct voltage level. Systems need to be protected from power loss, power degradation, and even from too much power, all of which can damage equipment. Common causes of voltage variation include lightning; damage to overhead lines from storms, trees, birds, or animals; vehicles striking poles or equipment; and load changes or equipment failure on the network. Heat waves can also contribute to power interruptions because the demand in electricity (that is, air conditioners) can sometimes exceed supply. The variation may be minor or significant.

Power fluctuations are categorized by changes in voltage and power loss. Figure 7-1 shows the difference between a ***power surge*** and a ***power spike***.

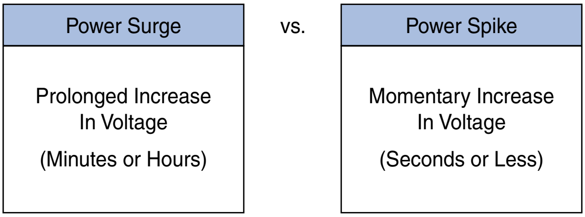


FIGURE 7-1 Power Surge vs. Power Spike

Figure 7-2 shows the difference between a ***brownouts*** and a ***sag***.

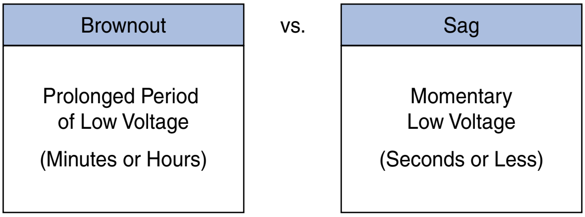


FIGURE 7-2 Brownout vs. Sag

Figure 7-3 shows the difference between a ***blackout*** and a ***fault***.

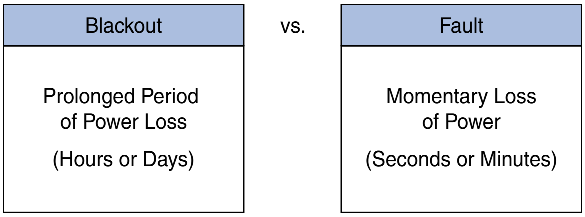


FIGURE 7-3 Blackout vs. Fault

Companies can install protective devices to help guard their premises and assets, such as installing surge protection equipment, line filters, isolation transformers, voltage regulators, power conditioners, uninterruptible power supplies (UPSs), and back-up power supplies or generators. These power protection devices can condition the feed for consistency, provide continuous power for critical systems, and manage a controlled shutdown in the event of total loss of power.

In Practice

Power Consumption Policy

Synopsis: Power conditioning and redundancy protections must be in place to maintain the availability and performance of information systems and infrastructure. Power consumption should be minimized.

Policy Statement:

- The company is committed to sustainable computing and the minimization of power consumption.
- All computing devices purchased must be Energy Star (or equivalent)–certified.
- All computing devices must be configured in power saver mode unless the setting degrades performance.
- A biannual assessment must be conducted by the Office of Facilities Management to determine the best method(s) to provide clean, reliable data center power.

- Data center equipment must be protected from damage caused by power fluctuations or interruptions.
- Data center power protection devices must be tested on a scheduled basis for functionality and load capacity. A log must be kept of all service and routine maintenance.
- Data center generators must be tested regularly according to manufacturer's instructions. A log must be kept of all service and routine maintenance.

How Dangerous Is Fire?

Imagine the impact of a data center fire—equipment and data irrevocably destroyed, internal communications damaged, and external connectivity severed. On November 2017, Data Center Dynamics reported that a faulty battery in a UPS caused a fire in a health center in Cairns, Australia, causing two hospitals and several of the city's health service systems to fail.

Fire protection is composed of the three elements shown in Figure 7-4.

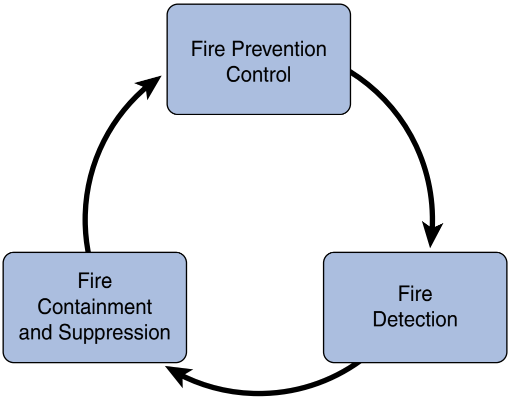


FIGURE 7-4 Fire Protection Elements

Active and passive ***fire prevention controls*** are the first line of defense. Fire prevention controls include hazard assessments and inspections, adhering to building and construction codes, using flame-retardant materials, and proper handling and storage procedures for flammable/combustible materials. ***Fire detection*** is recognizing that there is a fire. Fire detection devices can be smoke activated, heat activated, or flame activated. ***Fire containment and suppression*** involve actually responding to the fire. Containment and suppression equipment is specific to fire classification. Data center environments are typically at risk of Class A, B, or C fires:

- **Class A:** Fire with combustible materials as its fuel source, such as wood, cloth, paper, rubber, and many plastics

- **Class B:** Fire in flammable liquids, oils, greases, tars, oil-based paints, lacquers, and flammable gases
- **Class C:** Fire that involves electrical equipment
- **Class D:** Combustibles that involve metals

Facilities must comply with standards to test fire-extinguishing methods annually to validate full functionality.

The best-case scenario is that data centers and other critical locations are protected by an automatic fire-fighting system that spans multiple classes. Like all other major investments, it's prudent to do a cost/benefit analysis before making a decision. In any emergency situation, human life always takes precedence. All personnel should know how to quickly and safely evacuate an area.

In Practice

Data Center and Communications Facilities Environmental Safeguards Policy

Synopsis: Data center and communications facilities must have controls designed to minimize the impact of power fluctuations, temperature, humidity, and fire.

Policy Statement:

- Smoking, eating, and drinking are not permitted in data center and communications facilities.
- Servers and communications equipment must be located in areas free from physical danger.
- Servers and communications must be protected by uninterruptable power supplies and back-up power sources.
- Appropriate fire detection, suppression, and fighting equipment must be installed and/or available in all data center and communications facilities.
- Appropriate climate control systems must be installed in all data center and communications facilities.
- Emergency lighting must engage automatically during power outages at all data center and communications facilities.
- The Office of Facilities Management is responsible for assessing the data center and communications facilities environmental requirements and providing the recommendations to the COO.
- The Office of Facilities Management is responsible for managing and maintaining the data center and communications facilities' climate-control, fire, and power systems.

What About Disposal?

What do servers, workstations, laptops, tablets, smartphones, firewalls, routers, copiers, scanners, printers, memory cards, cameras, and flash drives have in common? They all store data that should be permanently removed before handing down, recycling, or discarding.

The data can be apparent, hidden, temporary, cached, browser-based, or metadata:

- ***Apparent data files*** are files that authorized users can view and access.
- ***Hidden files*** are files that the operating system by design does not display.
- ***Temporary files*** are created to hold information temporarily while a file is being created.
- A ***web cache*** is the temporary storage of web documents, such as HTML pages, images, and downloads.
- A ***data cache*** is the temporary storage of data that has recently been read and, in some cases, adjacent data areas that are likely to be accessed next.
- ***Browser-based data*** includes the following items:
  - Browsing history, which is the list of sites visited
  - Download history, which is the list of files downloaded
  - Form history, which includes the items entered into web page forms
  - Search bar history, which includes items entered into the search engines
  - Cookies, which store information about websites visited, such as site preferences and login status
- ***Metadata*** is details about a file that describes or identifies it, such as title, author name, subject, and keywords that identify the document's topic or contents.

Removing Data from Drives

A common misconception is that deleting a file will permanently remove its data. ***Deleting*** (or trashing) a file removes the operating system pointer to the file. ***Formatting*** a disk erases the operating system address tables. In both cases, the files still reside on the hard drive, and system recovery software can be used to restore the data. To give you an idea of how easy it is to recover information from a formatted hard drive, simply Google the phrase "data recovery" and see what comes back to you. Utilities are available for less than $50 that are quite capable of recovering data from formatted drives. Even if a drive has been formatted and a new operating system installed, the data is recoverable.

NIST Special Publication 800-88 Revision 1 defines ***data destruction*** as “the result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.” There are two methods of permanently removing data from a drive—disk wiping (also known as scrubbing) and degaussing. The ***disk wiping*** process will overwrite the master boot record (MBR), partition table, and every sector of the hard drive with the numerals 0 and 1 several times. Then the drive is formatted. The more times the disk is overwritten and formatted, the more secure the disk wipe is. The government medium security standard (DoD 5220.22-M) specifies three iterations to completely overwrite a hard drive six times. Each iteration makes two write passes over the entire drive; the first pass inscribes ones (1) over the drive surface and the second inscribes zeros (0) onto the surface. After the third iteration, a government-designated code of 246 is written across the drive, and then it is verified by a final pass that uses a read-verify process. There are several commercially available applications that follow this standard. Disk wiping does not work reliably on solid-state drives, USB thumb drives, compact flash, and MMC/SD cards.

Degaussing is the process wherein a magnetic object, such as a computer tape, hard disk drive, or CRT monitor, is exposed to a magnetic field of greater, fluctuating intensity. As applied to magnetic media, such as video, audio, computer tape, or hard drives, the movement of magnetic media through the degaussing field realigns the particles, resetting the magnetic field of the media to a near-zero state, in effect erasing all the data previously written to the tape or hard drive. In many instances, degaussing resets the media to a like-new state so that it can be reused and recycled. In some instances, this simply wipes the media in preparation for safe and secure disposal. The National Security Agency (NSA) approves powerful degaussers that meet their specific standards and that in many cases utilize the latest technology for top-secret erasure levels.

Cryptographic Erase is a technique that uses the encryption of target data by enabling sanitization of the target data’s encryption key. This is done to leave only the cipher text on the media and preventing read-access, because no one should have the encryption key. It is common for storage manufacturers to include integrated encryption and access control capabilities, also known as self-encrypting drives (SEDs). SEDs feature always-on encryption that ensures that all data in the storage device is encrypted. In practice, cryptographic erase can be executed in a fraction of a second. This is a great benefit because nowadays other sanitization methods take more time in large storage devices. Cryptographic erase can also be used in addition to other data destruction methods. You should not use cryptographic erase to sanitize data if the encryption was enabled after sensitive data was stored on the device without having been sanitized first. In addition, you should not use cryptographic erase if you are not certain if sensitive data was stored on the device without being sanitized prior to encryption.

Destroying Materials

The objective of physical ***destruction*** is to render the device and/or the media unreadable and unusable. Devices and media can be crushed, shredded, or, in the case of hard drives, drilled in several locations perpendicular to the platters and penetrating clear through from top to bottom.

Cross-cut shredding technology, which reduces material to fine, confetti-like pieces, can be used on all media, ranging from paper to hard drives.

It is common for organizations to outsource the destruction process. Companies that offer destruction services often have specialized equipment and are cognizant of environmental and regulatory requirements. The downside is that the organization is transferring responsibility for protecting information. The media may be transported to off-site locations. The data is being handled by non-employees over whom the originating organization has no control. Selecting a destruction service is serious business, and thorough due diligence is in order.

Both in-house and outsourced destruction procedures should require that an unbroken predestruction ***chain of custody*** be maintained and documented and that an itemized post-destruction certificate of destruction be issued that serves as evidence of destruction in the event of a privacy violation, complaint, or audit. NIST Special Publication 800-88 Revision 1 mentions that destructive techniques also render a "device purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing."

In Practice

Secure Disposal Policy

Synopsis: All media must be disposed of in a secure and environmentally sound manner.

Policy Statement:

- The Office of Facilities Management and the Office of Information Security are jointly responsible for determining the disposal standards for each classification of information.
- Devices or media containing "protected" or "confidential" information must not be sent off-site for repair and/or maintenance.
- The standards for the highest classification must be adhered to when the device or media contains multiple types of data.
- A chain of custody must be maintained for the destruction of "protected" and "confidential" information.
- A certificate of destruction is required for third-party destruction of devices or media that contains "protected" and "confidential" information.
- Disposal of media and equipment will be done in accordance with all applicable state and federal environmental disposal laws and regulations.

Stop, Thief!

According to the Federal Bureau of Investigation (FBI), on average, a laptop is stolen every 53 seconds, and one in ten individuals will have their laptop stolen at some point. The recovery statistics of stolen laptops is even worse, with only 3% ever being recovered. This means 97% of laptops stolen will never be returned to their rightful owners. The Ponemon Institute has conducted several studies and reported that almost half of laptops were lost or stolen off-site (working from a home office or hotel room) and one third were lost or stolen in travel or transit. The statistics for mobile phones and tablets is even worse.

The cost of lost and stolen devices is significant. The most obvious loss is the device itself. The cost of the device pales in comparison to the cost of detection, investigation, notification, after-the-fact response, and economic impact of lost customer trust and confidence, especially if the device contained legally protected information. The Ponemon Institute "2017 Cost of Data Breach Study: Global Overview" (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN) calculated the average business cost of a breach in the United States to be $141 per record across all industries.

Consider this scenario: A laptop valued at $1,500 is stolen. A file on the laptop has information about 2,000 individuals. Using the Ponemon conclusion of $141 per record, the cost of the compromise would be $282,000! That cost doesn't include potential litigation or fines.

Additional examples of things that are attractive to thieves are modern portable media theft, such as thumb or pen drives and SD cards. This is why it is important that you have a good asset inventory. In Chapter 5, "Asset Management and Data Loss Prevention," you learned that asset management is crucial. In addition, you learned that every information asset must be assigned an owner. The success of an information security program is directly related to the defined relationship between the data owner and the information. In the best-case scenario, the data owner also functions as a security champion enthusiastically embracing the goals of confidentiality, integrity, and availability (CIA).

You should also have an established and effective process for individuals to report lost or stolen devices. Additionally, you should have mitigations in place in case of theft. These mitigations include encryption and remote wipe capabilities for mobile devices. Typically, remote wipe is a function of a mobile device management (MDM) application.

In Practice

Mobile Device and Media Security

Synopsis: Safeguards must be implemented to protect information stored on mobile devices and media.

Policy Statement:

- All company-owned and employee-owned mobile devices and media that store or have the potential to store information classified as “protected” or “confidential” must be encrypted.
- Whenever feasible, an antitheft technology solution must be deployed that enables remote locate, remote lock, and remote delete/wipe functionality.
- Loss or theft of a mobile device or media must be reported immediately to the Office of Information Security.

FYI: Small Business Note

Two physical security issues are specific to small business and/or remote offices: location and person identification. A majority of small business and remote offices are located in multitenant buildings, where occupants do not have input into or control of perimeter security measures. In this case, the organization must treat their entry doors as the perimeter and install commensurate detective and preventative controls. Often, tenants are required to provide access mechanisms (for example, keys, codes) to building personnel, such as maintenance and security. Unique entry codes should be assigned to third-party personnel so that entry can be audited. Rarely are employee identification badges used in a small office. This makes it all the more important that visitors be clearly identified. Because there is little distinction between public and private spaces, visitors should be escorted whenever they need to go on the premises.

Summary

The objective of physical and environmental security is to prevent unauthorized access, damage, and interference to business premises and equipment. In this chapter, with a focus on the physical environment, we discussed the three elements to security—obstacles that deter trivial attackers and delay serious ones, detection systems that make it more likely that the attack will be noticed, and a response capability to repel or catch attackers. We began at the security perimeter, worked our way gradually inward to the data center, and then back out to mobile devices. Starting at the perimeter, we saw the importance of having a layered defense model as well as incorporating CPTED (crime prevention through environmental design) concepts. Moving inside the building, we looked at entry controls and the challenge of authorized access and identification. We acknowledged that not all access is equal. Workspaces and areas need to be classified so that levels of access can be determined and appropriate controls implemented. Equipment needs to be protected from damage, including natural disasters, voltage variations (such as surges, brownouts, and blackouts), fire, and theft. Purchasing Energy Star–certified equipment and proactively reducing energy consumption supports the long-term security principle of availability.

We explored the often-overlooked risks of device and media disposal and how important it is to permanently remove data before handing down, recycling, or discarding devices. Even the most innocuous devices or media may contain business or personal data in metadata, hidden or temporary files, web or data caches, or the browser history. Deleting files or formatting drives is not sufficient. DoD-approved disk-wiping software or a degaussing process can be used to permanently remove data. The most secure method of disposal is destruction, which renders the device and/or the media unreadable and unusable.

Mobile devices that store, process, or transmit company data are the newest challenge to physical security. These devices travel the world and in some cases are not even company-owned. Threats run the gamut from nosy friends and colleagues to targeted theft. The detection, investigation, notification, and after-the-fact response cost of a lost or stolen mobile device is astronomical. The economic impact of lost customer trust and confidence is long-lasting. Encryption and antitheft technology solutions that enable remote locate, remote lock, and remote delete/wipe functionality must be added to the protection arsenal.

Physical and environmental security policies include perimeter security, entry controls, workspace classification, working in secure areas, clean desk and clean screen, power consumption, data center and communications facilities environmental safeguards, secure disposal, and mobile device and media security.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following groups should be assigned responsibility for physical and environmental security?

   A. Facilities management

   B. Information security management

   C. Building security

   D. A team of experts including facilities, information security, and building security

2. Physical and environmental security control decisions should be driven by a(n) ___________.

   A. educated guess

   B. industry survey

   C. risk assessment

   D. risk management

3. Which of the following terms best describes CPTED?

   A. Crime prevention through environmental design

   B. Crime prevention through environmental designation

   C. Criminal prevention through energy distribution

   D. Criminal prosecution through environmental design

4. The design of a secure site starts with the _________.

   A. natural surveillance

   B. territorial reinforcement

   C. natural access control

   D. location

5. Which of the following models is known as the construct that if an intruder can bypass one layer of controls, the next layer of controls should provide additional deterrence or detection capabilities?

   A. Layered defense model

   B. Perimeter defense model

   C. Physical defense model

   D. Security defense model

6. The mere fact that an area appears to be secure is in itself a ___________.

   A. deterrent
   B. layer
   C. defense
   D. signature

7. Best practices dictate that data centers should be _____________.

   A. well marked
   B. located in urban areas
   C. inconspicuous and unremarkable
   D. built on one level

8. Which of the following would be considered a "detection" control?

   A. Lighting
   B. Berms
   C. Motion sensors
   D. Bollards

9. Badging or an equivalent system at a secure facility should be used to identify ____________.

   A. everyone who enters the building
   B. employees
   C. vendors
   D. visitors

10. Which of the following statements best describes the concept of shoulder surfing?

    A. Shoulder surfing is the use of a keylogger to capture data entry.
    B. Shoulder surfing is the act of looking over someone's shoulder to see what is on a computer screen.
    C. Shoulder surfing is the act of positioning one's shoulders to prevent fatigue.
    D. None of the above.

11. The term BYOD is used to refer to devices owned by ____________.

    A. the company
    B. a vendor
    C. the employee
    D. a contractor

12. Which of the following statements is *not* true about data center best practices?

    A. Data center equipment must be protected from damage caused by power fluctuations or interruptions.

    B. Data center power protection devices must be tested on a scheduled basis for functionality and load capacity.

    C. Data center generators must be tested regularly according to manufacturer's instructions.

    D. You can optionally log all service and routine maintenance.

13. Which of the following terms best describes a prolonged increase in voltage?

    A. Power spike

    B. Power surge

    C. Power hit

    D. Power fault

14. Common causes of voltage variations include ______________.

    A. lightning, storm damage, and electric demand

    B. using a power conditioner

    C. turning on and off computers

    D. using an uninterruptable power supply

15. Adhering to building and construction codes, using flame-retardant materials, and properly grounding equipment are examples of which of the following controls?

    A. Fire detection controls

    B. Fire containment controls

    C. Fire prevention controls

    D. Fire suppression controls

16. A Class C fire indicates the presence of which of the following items?

    A. Electrical equipment

    B. Flammable liquids

    C. Combustible materials

    D. Fire extinguishers

17. Confidential data can reside on which of the following items?

    A. Smartphones

    B. Cameras

    C. Scanners

    D. All of the above

18. Which of the following data types includes details about a file or document?

    A. Apparent data

    B. Hidden data

    C. Metadata

    D. Cache data

19. URL history, search history, form history, and download history are stored by the device ____________.

    A. operating system

    B. browser

    C. BIOS

    D. ROMMON

20. Which of the following statements about formatting a drive is not true?

    A. Formatting a drive creates a bootable partition.

    B. Formatting a drive overwrites data.

    C. Formatting a drive fixes bad sectors.

    D. Formatting a drive permanently deletes files.

EXERCISES

EXERCISE 7.1: Researching Data Destruction Services

1. Research companies in your area that offer data destruction services.
2. Document the services they offer.
3. Make a list of questions you would ask them if you were tasked with selecting a vendor for data destruction services.

EXERCISE 7.2: Assessing Data Center Visibility

1. Locate the data center at your school or workplace.
2. Is the facility or area marked with signage? How easy was it to find? What controls are in place to prevent unauthorized access? Document your findings.

EXERCISE 7.3: Reviewing Fire Containment

1. Find at least three on-campus fire extinguishers (do not touch them). Document their location, what class fire they can be used for, and when they were last inspected.
2. Find at least one fire extinguisher (do not touch it) in your dorm, off-campus apartment, or home. Document the location, what class fire it can be used for, and when it was last inspected.

EXERCISE 7.4: Assessing Identification Types

1. Document what type of identification is issued to students, faculty, staff, and visitors at your school. If possible, include pictures of these types of documentation.
2. Describe the process for obtaining student identification.
3. Describe the procedure for reporting lost or stolen identification.

EXERCISE 7.5: Finding Data

1. Access a public computer in either the library, a computer lab, or a classroom.
2. Find examples of files or data that other users have left behind. The files can be apparent, temporary, browser based, cached, or document metadata. Document your findings.
3. What should you do if you discover “personal” information?

PROJECTS

PROJECT 7.1: Assessing Physical and Environmental Security

1. You are going to conduct a physical assessment of a computing device you own. This could be a desktop computer, a laptop, a tablet, or a smartphone. Use the following table as a template to document your findings. You can add additional fields.

Device Description		**Laptop Computer**							
							Safeguard		
Threats/ Danger	Impact	Safeguard 1	Safeguard 2	Safeguard 3	Assessment	Recommendation	Initial Cost	Annual Cost	Cost/Benefit Analysis
Lost or forgotten	Need laptop for schoolwork	Pink case	Labeled with owner's contact info		Inadequate	Install remote find software	$20.00	$20.00	$20 per year vs. the cost of replacing the laptop

2. Determine the physical and environmental dangers (threats); for example, losing or forgetting your laptop at school. Document your findings.
3. For each danger (threat), identify the controls that you have implemented; for example, your case is pink (recognizable) and the case and laptop are labeled with your contact information. It is expected that not all threats will have corresponding safeguards. Document your findings.
4. For threats that do not have a corresponding safeguard or ones for which you feel the current safeguards are inadequate, research the options you have for mitigating the danger. Based on your research, make recommendations. Your recommendation should include initial and ongoing costs. Compare the costs of the safeguard to the cost impact of the danger. Document your findings.

PROJECT 7.2: Assessing Data Center Design

1. You have been tasked with recommending environmental and physical controls for a *new* data center to be built at your school. You are expected to present a report to the Chief Information Officer. The first part of your report should be a synopsis of the importance of data center physical and environmental security.
2. The second part of your report should address three areas: location, perimeter security, and power.
   a. Location recommendations should include where the data center should be built and a description of the security of the surrounding area (for example, location-based threats include political stability, susceptibility to terrorism, the crime rate, adjacent buildings, roadways, pedestrian traffic, flight paths, utility stability, and vulnerability to natural disasters).
   b. Access control recommendations should address who will be allowed in the building and how they will be identified and monitored.
   c. Power recommendations should take into account power consumption as well as normal and emergency operating conditions.

PROJECT 7.3: Securing the Perimeter

1. The security perimeter is a barrier of protection from theft, malicious activity, accidental damage, and natural disaster. Almost all buildings have multiple perimeter controls. We have become so accustomed to perimeter controls that they often go unnoticed (that is, security guards). Begin this project with developing a comprehensive list of perimeter controls.
2. Conduct a site survey by walking around your city or town. You are looking for perimeter controls. Include in your survey results the address of the building, a summary of building occupants, type(s) of perimeter controls, and your opinion as to the effectiveness of the controls. To make your survey valid, you must include at least 10 properties.
3. Choose one property to focus on. Taking into consideration the location, the depth of security required by the occupants, and the geography, comment in detail on the perimeter controls. Based on your analysis, recommend additional physical controls to enhance perimeter security.

Case Study

Physical Access Social Engineering

In your role of ISO at Anywhere USA University Teaching Hospital, you commissioned an independent security consultancy to test the hospital's physical security controls using social engineering impersonation techniques. At the end of the first day of testing, the tester submitted a preliminary report.

Physical Access to Facilities

Dressed in blue scrubs, wearing a stethoscope, and carrying a clipboard, the tester was able to access the lab, the operating room, and the maternity ward. In one case, another staff member buzzed him in. In the two other cases, the tester walked in with other people.

Physical Access to the Network

Dressed in a suit, the tester was able to walk into a conference room and plug his laptop into a live data jack. Once connected, he was able to access the hospital's network.

Physical Access to a Computer

Wearing a polo shirt with a company name, the tester was able to sit down at an unoccupied office cubicle and remove a hard disk from a workstation. When questioned, he answered that he had been hired by John Smith, IT Manager, to repair the computer.

Physical Access to Patient Files

Wearing a lab coat, the tester was able to walk up to a printer in the nursing station and remove recently printed documents.

Based on these findings, you request that the consultancy suspend the testing. Your immediate response is to call a meeting to review the preliminary report.

1. Determine who should be invited to the meeting.
2. Compose a meeting invitation explaining the objective of the meeting.
3. Prepare an agenda for the meeting.
4. Identify what you see as the most immediate issues to be remediated.

References

Regulations Cited

DoD 5220.22-M: National Industrial Security Program Operating Manual, February 28, 2006, revised March 28, 2013.

Other References

“About Energy Star,” Energy Star, accessed 04/2018, https://www.energystar.gov.

Amazon Web Services Physical Security Whitepaper, accessed 04/2018, https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

The Ponemon Institute, “2017 Cost of Data Breach Study: Global Overview,” accessed 04/2018, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN.

Destruct Data, “Department of Defense (DoD) Media Sanitization Guidelines 5220.22M,” accessed 04/2018, http://www.destructdata.com/dod-standard/.

Bray, Megan, “Review of Computer Energy Consumption and Potential Savings,” December 2006, accessed 04/2018, www.dssw.co.uk/research/computer_energy_consumption.html.

“Efficiency: How We Do It,” Google, accessed 04/2018, https://www.google.com/about/datacenters/efficiency/internal/index.html#temperature.

“Facilities Services Sustainable Computing Guide,” Cornell University, accessed 04/2018, http://www.ictliteracy.info/rf.pdf/FSSustainableComputingGuide.pdf.

"Foundations Recovery Network Notifying Patients After a Laptop with PHI Was Stolen from an Employee's Car," PHIprivacy.net, June 24, 2013, accessed 04/2018, https://www.databreaches.net/foundations-recovery-network-notifying-patients-after-a-laptop-with-phi-was-stolen-from-an-employees-car/.

"Google Data Centers," Google.com, accessed 04/2018, https://www.google.com/about/datacenters.

Jeffery, C. Ray. 1977. *Crime Prevention Through Environmental Design*, Second Edition, Beverly Hills: Sage Publications.

"Your Guide To Degaussers," Degausser.com, accessed 04/2018, http://degausser.com/.

"Data Center Battery Incident Causes Fire in Australian Hospital," Data Center Dynamics, accessed 04/2018, http://www.datacenterdynamics.com/content-tracks/security-risk/data-center-battery-incident-causes-fire-in-australian-hospital/99357.fullarticle.

Index

Numbers

7–11, data breach of, 556

800 series Special Publications (NIST), 84

1800 series Special Publications (NIST), 84

27000 series standards (ISO/IEC)

- domains
  - Access Control, 88–89, 295
  - Asset Management, 88, 145
  - Business Continuity Management, 91, 427
  - Communications Security, 90, 237
  - Compliance Management, 92, 504
  - Cryptography, 89
  - Human Resources Security Management, 88, 179
  - Information Security Incident Management, 91, 369, 387
  - Information Security Policies, 87
  - Information Systems Acquisition, Development, and Maintenance, 91, 339
  - Operations Security, 90, 237
  - Organization of Information Security, 87–88
  - overview, 86–87
  - Physical and Environmental Security, 89–90, 209
  - Supplier Relationship, 91
- history of, 86
- overview, 85, 104

31000 series standards (ISO/IEC), 104

A

ABAC (attribute-based access controls), 306

ABCP (Associate Business Continuity Professional), 439

acceptable use policy, 108, 191–192

accepting risk, 124

access control. *See also* authentication

- accounting, 306
- ACLs (access control lists), 303
- authorization 295, 303–307
- defined, 295
- email, 264
- failed access, 325
- HIPAA (Health Insurance Portability and Accountability Act), 520–522
- identification, 295–303
- infrastructure access controls, 307–311
- intentional unauthorized access or use, 372–373
- ISO/IEC guidance, 295
- layered border security, 265, 311–315, 347–348
- monitoring, 325–326
- NIST Special Publications, 295
- overview, 294
- PCI DSS (Payment Card Industry Data Security Standard), 556–558
- physical, 213–216
- principle of least privilege, 297–298
- remote access security, 317–321
  - mutual authentication, 318–319
  - NAC (Network Access Control), 319

remote access portals, 318
sample policy, 319–320
teleworking, 320–321
VPNs (virtual private networks), 318
security breach assessment, 336
security posture, 296–297
small business considerations, 326
successful access, 325
terminology, 295–296
user, 321–324
Access Control domain (ISO 27002 standard), 88–89
access control lists (ACLs), 303
account data, 548
Account Data Compromise Recovery (ADCR), 567
accountability, 81
accounting, 81, 306
ACLs (access control lists), 303
acquirers, 547
Active Directory Group Policy, 40
active voice, 47–48
activity monitoring. *See* logs
adaptable policies, 14–15
Adaptive tier (NIST Framework), 593–594
ADCR (Account Data Compromise Recovery), 567
address space layout randomization (ASLR), 349
addressable implementations, 507
addresses
IP (Internet Protocol) 161–162, 312
logical, 161–162
randomization, 349
spoofing, 374
Adelphia, 183
Adjucation phase (security clearance), 186
administrative account controls, 323–324
administrative notations, 59
administrative safeguards (HIPAA), 508–516
adoption of policies, 26
Advanced Encryption Standard (AES), 351–352
Advanced Malware Protection (AMP), 10, 297
advanced persistent threats (APTs), 250–251
Advanced Research Project Agency (ARPA), 261–262
AES (Advanced Encryption Standard), 351–352
aggregation, log, 271
agreements, 191–192
AICPA (American Institute of CPAs), 275
algorithms, Luhn, 549–550
Alisuretove, Elvin, 558
alpha phase, 343
Amazon Web Services (AWS), 210
American Institute of CPAs (AICPA), 275
American National Standards Institute (ANSI), 114
Americans with Disabilities Act, 185
AMP (Advanced Malware Protection), 10, 297
analyzing logs, 271–273
ANSI (American National Standards Institute), 114
antivirus (AV) software, 254–258
apparent data files, 221
appetite for risk, 126
application development policy, 349–350
Application layer (OSI model), 256
Application phase (security clearance), 186
application security, 10
Approved Scanning Vendors (ASVs), 547, 565
approving policies, 24
APTs (advanced persistent threats), 250–251
Army Clarity Index, 48–49
ARPA (Advanced Research Project Agency), 261–262
ARPANET, 261–262
ASLR (address space layout randomization), 349
assessments
business continuity, 433–436
defined, 477
PCI DSS compliance, 564–565
risk, 127–131, 141
security breach, 336

Asset Management domain (ISO 27002 standard), 88, 145

assets

- business continuity, 430–431
- defined, 9–11, 145
- disposing of, 162
- DLP (data loss prevention), 164–166
- examples of, 145–146
- handling standards, 157–159
- importance of, 144–145
- information classification, 148–156, 176–177
- inventory, 159–163
- labeling, 156
- NIST Cybersecurity Framework, 145
- physical and environmental security, 231–232
- removing, 162
- responsibility for, 146–148

assigned security responsibility (HIPAA), 509

Associate Business Continuity Professional (ABCP), 439

assurance, defined, 81

assurance tests, 477

ASVs (Approved Scanning Vendors), 547, 565

asymmetric keys, 353

attacks. *See also* malware

- botnets, 399
- DDoS (distributed denial-of-service), 60, 79–82, 373
- DoS (denial-of-service), 79–82, 265, 373
- Equifax breach, 499
- hacktivism, 76, 77
- HealthNow Networks breach, 543–544
- inappropriate usage, 375
- Indiana Medicaid breach, 543–544
- intentional unauthorized access or use, 372–373
- low-bandwidth, 374
- payment card data breaches, 555–556, 578–579

attainable policies, 14

attorney-client privilege, 75

attribute-based access controls, 306

audience analysis, 49

audits

- business continuity plan, 450
- defined, 114, 477
- HIPAA (Health Insurance Portability and Accountability Act), 522
- internal, 113
- regulatory requirements, 451
- reports, 275

authentication

- characteristic-based, 302
- defined, 81, 295
- HIPAA (Health Insurance Portability and Accountability Act), 522–523
- knowledge-based, 299–300
- multi-factor, 301, 303
- multilayer, 303
- out-of-band, 301
- OWASP (Open Web Application Security Project), 349
- ownership- or possession-based, 301
- PCI DSS (Payment Card Industry Data Security Standard), 557–558
- remote access, 318–319
- single-factor, 303

authenticity, cryptography and, 350

authority, IRTs (incident response teams), 396

authorization

- attribute-based access controls, 306
- authorization model, 303
- authorized entry, 213
- cybersecurity policies, 24
- defined, 81, 295, 303, 522–523
- discretionary access controls (DACs), 304
- HIPAA compliance standards, 510
- mandatory access controls (MACs), 304
- overview, 303–304
- of policies, 110
- RBACs (role-based access controls), 304, 305
- sample policy, 305, 306–307
- SOP documentation, 239

AV (antivirus) software, 254–258

availability, 78–79, 151. *See also* attacks

avoiding risk, 124

awareness, security, 194

Awareness and Training category (NIST Cybersecurity Framework), 589

AWS (Amazon Web Services), 210

B

backdoors, 61

background checks, 183–185, 213

backups, 258–261

Bad Rabbit, 252

badging systems, 213

Bank Service Company Act (BSCA), 478

banking regulations, 21

bankruptcies, employee screening and, 185

Bankruptcy Code, 185

baselines, 40–41

BCPs (business continuity plans), 436

BCT (Business Continuity Team), 437

Bell-Lapadula model, 148–149

benefits employee data, 187

beta phase, 343

BIA (business impact assessment), 433–436, 513

Biba model, 148–149

biometric-based authentication, 302

black box assurance tests, 477

BlackDuck, 392

blacklisting, 265, 315

blackouts, 218

blended threats, 255

blue teams, 316

border security, layered, 265, 311–315, 347–348

botnets, 81, 252, 373, 399

bots, 252

breach notifications. *See* data breach notifications

breaches. *See* attacks; incident response

bring your own device (BYOD), 217

brownouts, 217

browser-based data, 221

BSCA (Bank Service Company Act), 478

The Buckle, Inc, data breach of, 556

Buffet, Warren, 45

bulletins, ITL, 84

Bush, George W.9

business associates 505, 524–525, 528

business continuity

audits, 450

BCPs (business continuity plans), 436

BCT (Business Continuity Team), 437

disaster response plans, 440–448, 452, 460

emergency preparedness, 427, 430

maintenance, 450–451

NIST Cybersecurity Framework, 427

operational contingency plans, 444–445

overview, 426

regulatory requirements, 429–430

resilience, 428–429

risk management, 430–433

roles and responsibilities, 437–439

testing, 449–450

Business Continuity Booklet (FFIEC), 274

Business Continuity Management domain (ISO 27002 standard), 91, 427

Business Continuity Team (BCT), 437

Business Environment category (NIST Cybersecurity Framework), 587

business impact assessment (BIA), 433–436, 513

business-as-usual approach, 551–552

business/process level, framework implementation and, 594

BYOD (bring your own device), 217

C

C&A (certification and accreditation), 341

C&C (command and control) systems, 251–252, 440–441

caches, 221

California Security Breach Information Act, 19–20, 407

candidate application data, 182

capability maturity model (CMM), 115

cardholder data. *See* PCI DSS (Payment Card Industry Data Security Standard)

career development, 180

Caremark International, Inc.110

Carter, Jimmy, 45

CAs (Certification Authorities), 353

CAV2 codes, 549

CBCP (Certified Business Continuity Professional), 439

CCFP (Certified Cyber Forensics Professional) certification, 400

CCleaner, 257

CER (crossover error rate), 302

CERT (Computer Emergency Response Team), 108, 190

certificates, digital, 353–354, 355

certification and accreditation (C&A), 341

Certification Authorities (CAs), 353

certifications

- CBCP (Certified Business Continuity Professional), 439
- CCFP (Certified Cyber Forensics Professional), 400
- certification organizations, 617
- CFCP (Certified Functional Continuity Professional), 439
- CISAs (Certified Cybersecurity Auditors), 114
- verifying, 183

CEs (covered entities)

- breach notifications, 531
- business associate contracts, 524–526
- defined, 504

CFCP (Certified Functional Continuity Professional), 439

CFOs (Chief Financial Officers), 183

CFTC (Commodity Futures Trading Commission), 466

chain of custody, 223, 377, 400–401

chaining product security vulnerabilities, 391

championing policies, 25

change control, 243–247

change drivers, 117

characteristic-based authentication, 302

Chief Financial Officers (CFOs), 183

Chief Information Security Officers (CISOs), 49, 111–112

Chief Operating Officers. *See* COOs (Chief Operating Officers)

Chipotle, data breach of, 567

CIA triad. *See also* information classification

- availability, 78–79
- confidentiality, 74–77
- Five A's, 81
- integrity, 77–78
- overview, 73
- responsibility for, 82–83

CID codes, 549

cipher text, 350

CISAs (Certified Cybersecurity Auditors), 114

Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability, 76–77

Cisco Advanced Malware Protection (AMP), 10, 297

Cisco Cognitive Threat Analytics (CTA), 297

Cisco Computer Security Incident Response Teams. *See* CSIRTs (Cisco Computer Security Incident Response Teams)

Cisco Identity Service Engine (ISE), 40

Cisco Product Development Methodology (PDM), 392

Cisco Security Vulnerability Policy, 108, 248

Cisco Spark, 266

Cisco Talos, 252

Cisco WebEx Meetings Server Information Disclosure Vulnerability, 76–77

CISOs (Chief Information Security Officers), 49, 111–112

Citizenship and Immigration Services, Form I-9 Employment Eligibility Verification, 186–187

ClamAV, 255

Clarity Index (U.S. Army), 48–49

Clarke, Richard, 9

Class A-D fires, 219–220

classification. *See* information classification

clear desks and screens, 216

clearance, government, 186

client nodes, 353

Clinton, William, 9, 18, 46, 463

cloud computing, 165, 210, 259

CloudLock, 165

CMM (capability maturity model), 115

CNC (command and control) systems, 81–82

COBIT (Control Objectives for Information and Related Technologies), 118, 477

Code of Practice (ISO). *See* 27000 series standards (ISO/IEC)

cognitive passwords, 299–300

Cognitive Threat Analytics (CTA), 297

cold sites, 442

collaboration services, 266

Collector entity (syslog), 271

command and control (CnC) systems, 81–82, 251–252, 440–441

commercial off-the-shelf software. *See* COTS (commercial off-the-shelf software)

Commodity Futures Trading Commission (CFTC), 466

Common Vulnerability Scoring System (CVSS), 76–77, 387–390

Common Weakness Enumeration (CWE), 346

communications security. *See also* operations security

- change control, 243–247
- collaboration services, 266
- disaster response plans, 441
- email, 261–267
- NIST Cybersecurity Framework, 237
- overview, 24–25, 236–237
- recovery, 446
- SOPs (standard operating procedures), 238–243
- stakeholder communication, 595–596
- supply chain communication, 595–596
- threat intelligence and information sharing, 278–280

Communications Security domain (ISO 27002 standard), 90, 237

compliance management. *See* financial institutions, regulatory compliance for; health-care sector, regulatory compliance for

Compliance Management domain (ISO 27002 standard), 92, 504

Compliance Officers, 113

compliance risk, 472

components, policy

- administrative notations, 59
- definition section, 60–61
- enforcement clause, 58
- exceptions, 57–58
- exemption process, 57–58
- goals and objectives, 55–56
- introduction, 52–54
- policy heading, 54–55
- sample policy, 56–57
- table of, 51
- terms and definitions, 60–61
- version control, 51–52

CompTIA, 617

Computer Emergency Response Team. *See* CERT (Computer Emergency Response Team)

Confidential (C) information

- handling standards, 157
- national security information, 153
- private sector, 154

confidentiality

- confidentiality agreements, 191
- cryptography and, 350
- defined, 74–77
- FIPS-199 (Federal Information Processing Standard 199), 150
- legislation, 75

consolidated policies, 49–51

Constitution, as policy, 6

consumer information, 469

containment, eradication, and recovery phase (incident response), 382–383

containment, fire, 219

content filtering, 315

contingency plans, 436, 513–515

continuity of operations (COOP). ***See*** **business continuity**

contracts, service provider, 275–276

Control Objectives for Information and Related Technologies (COBIT), 118, 477

controls, 128

coordination centers, 393

COOs (Chief Operating Officers), 213, 215

Corporate Account Takeover Fraud Advisory, 487

corporate culture, 7–8

correlation, log, 271

COTS (commercial off-the-shelf software), 342–343

covered entities. ***See*** **CEs (covered entities)**

CPTED (Crime Prevention Through Environmental Design), 212

credit card data. ***See*** **PCI DSS (Payment Card Industry Data Security Standard)**

credit history, checking, 184

credit union case study, 35

Crime Prevention Through Environmental Design (CPTED), 212

criminal history, checking, 184, 185

critical infrastructure sectors, 2

crossover error rate (CER), 302

cryptographic erase, 222

cryptography, 89, 350–351

Cryptography domain (ISO 27002 standard), 89

CSD (Computer Security Division) of NIST, 83

CSF. ***See*** **NIST Cybersecurity Framework**

CSIRTs (Cisco Computer Security Incident Response Teams)

- establishing, 384
- GOSINT, 279
- national, 393

CTA (Cognitive Threat Analytics), 297

culture

- of compliance, 25
- corporate, 7–8

custodians, information, 82–83, 114, 194

custody, chain of, 223, 377, 400–401

customer information, 469

customer information systems, 469

CVC2 codes, 549

CVSS (Common Vulnerability Scoring System), 76–77, 387–390

CVV2 codes, 549

CWE (Common Weakness Enumeration), 346

cyber insurance, 125

“cyber” prefix, 9

Cyber Supply Chain Risk Management, 592–594

Cybersecurity Assessment Tool (FFIEC), 474–475

Cybersecurity Enhancement Act, 582

Cybersecurity Framework. ***See*** **NIST Cybersecurity Framework**

“Cybersecurity Framework: Intel’s Implementation Tools and Approach” (Intel), 606

cybersecurity policies. ***See*** **policies**

Cybersecurity Steering Committee, 113

Cybersecurity Workforce Framework (NICE), 194

CyberSeek, 205–206

D

DACs (discretionary access controls), 304

data at rest, 521

data breach notifications

- effectiveness of, 408
- HITECH (Health Information Technology for Economic and Clinical Health Act), 530–531
- public relations, 409–410
- regulatory requirements, 402–408
- sample policy, 409

data breaches. ***See*** **attacks; incident response**

data caches, 221

data classification, 75

Data Compromise Recovery Solution (DCRS), 567

data destruction, 222, 223

data disposal, 221–223

data exfiltration, 165

data extrusion, 165

data in motion, 523

data integrity, 78

Data Link layer (OSI model), 256

data loss prevention (DLP), 164–166

data replication and backups, 258–261

Data Security category (NIST Cybersecurity Framework), 589

data users, 114

DCRS (Data Compromise Recovery Solution), 567

DDoS (distributed denial-of-service) attacks, 60, 79–82, 373

De Palma, Brian, 77–78

deactivation, defined, 448

declassification of information, 156

decryption, 351

default allow, 296

default deny, 296

defense-in-depth strategy, 9–10, 253

defensive risk controls, 124

definitions, policy, 60–61

degaussing, 222

de-identification, 344

deleting files, 221

denial-of-service (DoS) attacks, 79–82, 265, 373

deny-all, 520

Department of Financial Services (New York), 20, 107

Department of Health and Human Services (HHS)

- HIPAA Security Series, 609–613
- HIPAA training, 529
- OCR (Office of Civil Rights), 19

Department of Homeland Security

- critical infrastructure sectors, 2
- Form I-9 Employment Eligibility Verification, 186–187

dependencies, service providers, 447

derivative classification, 153–154

Designated Entities Supplemental Validation (DESV), 561

designated incident handlers (DIHs), 395

desks, securing, 216

destruction of materials, 162, 223

DESV (Designated Entities Supplemental Validation), 561

Detect function (NIST Framework Core), 589–590

detection and analysis phase (incident response), 381–382

detection controls, 254

"Developing Effective Standard Operating Procedures" (Grusenmeyer), 242

development/acquisition phase (SDLC), 340–341

devices, mobile

- HIPAA compliance, 518–520
- physical security, 224–225

digital certificates, 353–354, 355

digital signatures, 351

DIHs (designated incident handlers), 395

Directive on Security of Network and Information Systems, 22, 121

Disaster Recovery Institute (DRI), 439, 617

disaster response plans. *See also* business continuity

- command and control centers, 440–441
- communication, 441
- disaster, defined, 427
- emergency preparedness, 430
- OEPs (occupant emergency plans), 441
- operational contingency plans, 444–445
- organizational structure, 440
- overview, 440
- recovery phase, 445–448
- relocation strategies, 441–443

resumption phase, 448
small business considerations, 452
social media and, 460
discretionary access controls (DACs), 304
disposal of data, 162, 221–223
disposal phase (SDLC), 341–342
disseminating cybersecurity policies, 25
distributed denial-of-service (DDoS) attacks, 60, 79–82, 373
distributed governance model, 111–114
DLP (data loss prevention), 164–166
DMZ, 308
doctor-patient privilege, 75
documentation
HIPAA compliance standards, 526
incident investigation, 398
domains, security, 73
DoS (denial-of-service) attacks, 79–82, 265, 373
downloaders, 253
DPPA (Drivers Privacy Protection Act), 184–185
DRI (Disaster Recovery Institute), 439, 617
drivers, change, 117
Drivers Privacy Protection Act (DPPA), 184–185
drives, removing data from, 221–222
dual control, 323
due diligence, 274–275
dummy data, 344
duties, segregation of, 323
duty of care, 110
dynamic data verification, 348

E

education. *See* training
educational credentials, verifying, 183
EER (equal error rate), 302
EFTA (Electronic Fund Transfer Act), 546–547
E-Government Act, 83–84
egress traffic, 311
Electronic Fund Transfer Act (EFTA), 546–547
electronic monitoring, 188–189
electronic protected health information (ePHI), 19, 504
email
controlling access to, 264
encryption, 262–263
history of, 261–262
hoaxes, 264
malware in, 263–264
metadata, 263
protocols, 262–263
sample policy, 267
servers, 265
user error, 264–265
emergency preparedness, 427, 430
employee agreements, 191–193
employee life cycle
insider threats, 190
onboarding, 187
orientation, 188–189
overview, 179–180
recruitment, 181–186
termination, 189–190
user provisioning, 187–188
employee training, 25, 194–195, 396
employment history, verifying, 183
enclave networks, 308
encryption
advantages of, 351–352
cardholder data, 554
CAs (Certification Authorities), 353
cipher text, 350
cryptography, 350
data at rest, 75
decryption, 351
defined, 350–351
digital certificates, 353–354, 355, 356
digital signatures, 351

email, 262–263
as evasion technique, 374
hashing, 351
keys, 351–356
message integrity, 351
mobile devices and, 224
PKI (Public Key Infrastructure), 353
randomware, 252
RAs (Registration Authorities), 353
regulatory requirements, 352

endorsed policies, 11–13

Energy Star certification, 218

enforceable policies, 15–16

enforcement clauses
HIPAA (Health Insurance Portability and Accountability Act), 532–533
HITECH (Health Information Technology for Economic and Clinical Health Act), 528–529
importance of, 26
policy, 58

ENISA (European Union Agency for Network and Information Security), 21

Enron, 183

entry, authorizing, 213

environmental security
access control 213–236
assessing, 231–232
cloud and, 210
data disposal, 221–223
equipment protection, 217
fire protection, 219–220
layered defense model, 210
mobile devices and media, 224–225
NIST Cybersecurity Framework, 209–210
NIST Special Publications, 209–210
overview, 208–209
physical access social engineering case study, 233–234
power protection, 217–219
site design, 211–213, 233
small business considerations, 225

ePHI (electronic protected health information), 19, 504

equal error rate (EER), 302

Equifax security breach, 12, 403, 499, 578–579

equipment protection, 217

erasing data, 221–222

EternalBlue, 252

European Union Agency for Network and Information Security (ENISA), 21

European Union Global Data Protection Regulation (GDPR), 22, 121, 184, 352

evaluating policies, 114–115

events, defined, 371

evidence handling
chain of custody, 223, 377, 400–401
cybersecurity forensic evidence, 377
digital forensic evidence, 377
forensic image files, 377
sample policy, 401–402
storage and retention, 401

examination, regulatory, 482–484

exceptions, policy, 57–58

executive level, framework implementation and, 594

Executive Order 13636, 582–583

exemption process, 57–58

exfiltration, data, 165

Exploit Wednesday, 248

Exploitability metrics (CVSS), 388–389

exploits. *See* malware

External Participation (NIST Cybersecurity Framework), 592–594

external product security vulnerabilities, 391–392

extrusion, data, 165

F

facilities
HIPAA compliance, 517
physical access control, 214–215

Facilities Management, Office of
fire protection policy, 220
power consumption policy and, 218
risk assessments conducted by, 213
visitor identification by, 214
workspace classifications, 215
facilities recovery, 446
FACTA (Fair and Accurate Credit Transaction Act of 2003), 185
failed access, 325
FAIR (Factor Analysis of Information Risk), 129–130
false acceptance error (FAR), 302
false negatives, 373–374
false positives, 373–374
false rejection error (FRR), 302
Family Educational Rights and Privacy Act (FERPA), 19, 107, 184
FAR (false acceptance error), 302
faults, 218
FBI (Federal Bureau of Investigation), 398–399, 487
FCBA (Fair Credit Billing Act), 546–547
FCRA (Fair Credit Reporting Act), 185
FDIC (Federal Deposit Insurance Corporation), 18, 21, 466
federal banking regulations. *See* financial institutions, regulatory compliance for
Federal Financial Institutions Examination Council. *See* FFIEC (Federal Financial Institutions Examination Council)
Federal Information Processing Standards. *See* FIPS (Federal Information Processing Standards)
Federal Information Security Management Act (FISMA), 107, 272, 369
Federal Plain Language Guidelines, 46–47
Federal Register, 467
Federal Reserve Bank (FRB), 18, 21, 466
Federal Trade Commission. *See* FTC (Federal Trade Commission)
FedRAMP (Federal Risk and Authorization Management Program), 266
feedback, soliciting, 26
FERPA (Family Educational Rights and Privacy Act), 19, 107, 184
FFIEC (Federal Financial Institutions Examination Council), 609–613
Cybersecurity Assessment Tool, 474–475
handbooks
Business Continuity Booklet, 274
Information Technology Examination, 474
Internet Banking Environment Guidance, 486–487
Outsourcing Technology Services, 478
overview, 451, 609–613
files, 221
filtering
content, 315
packets, 312–313
financial institutions, regulatory compliance for. *See also* GLBA (Gramm-Leach-Bliley Act)
audits, 451
BSCA (Bank Service Company Act), 478
business continuity, 429–430
compliance risk, 472
culture of compliance, 25
Glass-Steagall Act, 463
identity theft, 484–487, 499
Interagency Guidelines, 468–480
NY DFS Cybersecurity Regulation, 480–482
PCI DSS (Payment Card Industry Data Security Standard), 107, 120, 272, 547–567, 578–579
regulatory examination, 482–484
terminology, 469
Financial Modernization Act. *See* GLBA (Gramm-Leach-Bliley Act)
Financial Services Information Sharing and Analysis Center (FS-ISAC), 384, 487
fines
for HITECH noncompliance, 528–529
for PCI DSS noncompliance, 568
FIPS (Federal Information Processing Standards), 83–84, 150–152

fire protection, 219–220

firewalls, 255, 311–314, 553

FIRST (Forum of Incident Response and Security Teams), 249, 393, 617

FISMA (Federal Information Systems Management Act), 107, 272, 369

Five A's of information security, 81

FOIA (Freedom of Information Act), 150

forensic analysis

- CCFP (Certified Cyber Forensics Professional) certification, 400
- chain of custody, 223, 377, 400–401
- evidence storage and retention, 401
- process, 399–400
- sample policy, 401–402

forensic image files, 377

Form I-9 Employment Eligibility Verification, 187

Form W-4 Employee's Withholding Allowance Certificate, 186–187

formatting

- files, 221
- policies, 49–51

Forum of Incident Response and Security Teams (FIRST), 249, 393, 617

fragmentation, 374

Framework for Improving Critical Infrastructure Cybersecurity. *See* NIST Cybersecurity Framework

Fraud Advisory for Business: Corporate Account Takeover, 487

FRB (Federal Reserve Bank), 18, 21, 466

Freedom of Information Act (FOIA), 150

FRR (false rejection error), 302

FS-ISAC (Financial Services Information Sharing and Analysis Center), 384, 487

FTC (Federal Trade Commission)

- breach notification rules, 405
- GLBA (Gramm-Leach-Bliley Act) enforcement by, 18, 466
- responsibilities of, 464
- Safeguards Act, 467–468

full-scale testing, 450

functional exercises, 449

G

GDPR (General Data Protection Regulation), 22, 121, 184, 352

Glass-Steagall Act, 463

GLBA (Gramm-Leach-Bliley Act)

- components of, 463–465
- cybersecurity roles and responsibilities, 120
- Federal Register, 467
- financial institutions, defined, 463–464
- Glass-Steagall Act, 463
- Interagency Guidelines, 468–480
- log review, 272
- NY DFS Cybersecurity Regulation, 480–482
- overview, 18, 107, 462–463
- pretexting, 465
- Privacy Rule, 465
- regulatory examination, 482–484
- regulatory oversight, 465–466
- Safeguards Rule, 465, 467–468
- terminology, 469

Global Payments, Inc., data breach of, 556

global policies, 21–22

go live phase, 343

goals, policy, 55–56

GOSINT, 279

governance

- business continuity, 437
- defined, 105
- distributed model, 111–114
- NIST Cybersecurity Framework, 118–120, 587
- policy evaluation, 114–115
- policy revision, 117
- regulatory requirements, 107, 120–121
- strategic alignment, 105–107

government, role in cybersecurity policies. *See* regulatory requirements

Gramm-Leach-Bliley Act. *See* GLBA (Gramm-Leach-Bliley Act)

graphic format (SOPs), 241

Group Policy configuration (Windows), 40

group-based access, 511

Grusenmeyer, David, 242

guest networks, 308

guidelines, policy, 42

H

hacktivism, 76, 77

handling standards, 159–159

hardware assets, inventory of, 160

hashing, 351

heading, policy, 54–55

Health and Human Services. *See* Department of Health and Human Services (HHS)

Health Information Technology for Economic and Clinical Health Act. *See* HITECH (Health Information Technology for Economic and Clinical Health Act)

Health Insurance Portability and Accountability Act. *See* HIPAA (Health Insurance Portability and Accountability Act)

health plans, 504

health-care clearinghouses, 505

health-care providers, 504

health-care sector. *See* HIPPA (Health Insurance Portability and Accountability Act); HITECH (Health Information Technology for Economic and Clinical Health Act)

HealthNow Networks breach, 543–544

HealthSouth, 183

HHS. *See* Department of Health and Human Services (HHS)

hidden files, 221

hierarchical format (SOPs), 240–241

hierarchy, policy, 39, 109

high potential impact, 150

HIPAA (Health Insurance Portability and Accountability Act). *See also* HITECH (Health Information Technology for Economic and Clinical Health Act)
- administrative safeguards, 507–516
- compliance with, 599
- cybersecurity roles and responsibilities, 120
- data breach notifications, 404–405
- DHHS training, 529
- enforcement, 532–533
- HealthNow Networks breach, 543–544
- HIPAA Security Series, 609–613
- history of, 502–504
- implementation specifications, 507
- Indiana Medicaid breach, 543–544
- log review, 272
- objective of, 505–506
- Omnibus Rule, 527–528
- overview, 19, 107
- physical safeguards, 517–520
- technical safeguards, 520–527
- terminology, 504–505

HIPSs (host intrusion prevention systems), 255

HITECH (Health Information Technology for Economic and Clinical Health Act)
- breach notifications, 530–531
- business associates, 528
- data breach notifications, 404–405
- enforcement, 528–529
- history of, 502–504
- overview, 19
- subcontractors, 528

hoaxes, email, 264

Home Depot, data breach of, 556, 568, 578–579

Home screen (NIST CSF Reference Tool), 597

honoring the public trust, 8, 34

host intrusion prevention systems (HIPSs), 255

host security, 10

hot sites, 441

Hudson Bay, data breach of, 567

human resources
- business continuity, 438
- employee agreements, 191–193
- employee life cycle
  - insider threats, 190
  - onboarding, 187

orientation, 188–189

overview, 179–180

recruitment, 181–186

termination, 189–190

user provisioning, 187–188

insider threats, 190

NIST Cybersecurity Framework, 179

onboarding, 187

orientation, 188–189

overview, 178–180

recruitment, 181–186

SETA (Security Education, Training, and Awareness) model, 193–195

small business considerations, 195

termination, 189–190

user provisioning, 187–188

visitor credentialing by, 214

Human Resources Security Management domain (ISO 27002 standard), 88, 179

Hurricane Maria, 460

hybrid malware, 251

hyperlinks, 264

I

I-9 Form, 186–187

IC3 (Internet Crime Complaint Center), 487

ICA (International CPTED Association), 212

ICASI (Industry Consortium for Advancement of Security on the Internet), 249

identification

authentication

characteristic-based, 302

defined, 81, 295

HIPAA (Health Insurance Portability and Accountability Act), 522–523

knowledge-based, 299–300

multi-factor, 301, 303

multilayer, 303

out-of-band, 301

OWASP (Open Web Application Security Project), 349

ownership- or possession-based, 301

PCI DSS (Payment Card Industry Data Security Standard), 557–558

single-factor, 303

authorization, 306–307

defined, 295, 298

Identify function (NIST Framework Core), 587–588

identity management, 295–296

Identity Management, Authentication and Access Control category (NIST Cybersecurity Framework), 209, 588

Identity Service Engine (ISE), 40

identity theft, 484–487

Identity Theft Data Clearinghouse, 486

identity-based access, 511

IDSs (intrusion detection systems), 314–315

IEC (International Electrotechnical Commission), 85

IETF (Internet Engineering Task Force), 267–268, 318

IIHI (individually identifiable health information), 504

IMAP (Internet Message Access Protocol), 262

IMEI (International Mobile Equipment Identity) numbers, 549

impact, defined, 128

Impact metrics (CVSS), 389

implementation/operations level, framework implementation and, 594

implicit deny, 303

"Improving Critical Infrastructure Cybersecurity" (Executive Order 13636), 582–583

incident response. *See also* attacks

case study, 419–423

coordinators, 395

data breach notifications

effectiveness of, 408

HITECH (Health Information Technology for Economic and Clinical Health Act), 530–531

public relations, 409–410
regulatory requirements, 402–408
sample policy, 409
importance of, 20, 369–370
inappropriate usage, 375
incident classification, 372–375
incident definition, 370–372
incident severity levels, 375–376
information sharing, 384
investigation
cybersecurity forensic evidence, 377
digital forensic evidence, 377
documentation, 398
forensic analysis, 399–402
forensic image files, 377
law enforcement, 398–399
overview, 397
NIST Special Publications, 369
overview, 368
plans, 379–380
playbooks, 383–384
process, 381–383
preparation phase, 381
product security vulnerabilities
chaining, 391
internal versus external, 391–392
severity levels, 387–390
theoretical, 391
programs, 379–380
reporting, 376–378
tabletop exercises, 383–384
teams
authority, 396
CSIRTs (Cisco Computer Security Incident Response Teams), 385–387, 393–394
incident response providers, 394
MSSPs (Managed Security Service Providers), 394
personnel, 394–396
PSIRTs (Product Security Incident Response Teams), 387
training, 396
US-CERT (United States Computer Emergency Readiness Team), 370

inclusive policies, 16–17

Indiana Medicaid breach, 543–544

indicators of compromise (IOCs), 268, 291–292

individually identifiable health information (IIHI), 504

Industry Consortium for Advancement of Security on the Internet (ICASI), 249

information access management (HIPAA), 510–511

information assets. *See* assets

Information Assurance Framework (NIST), 83–84

information classification
Bell-Lapadula model, 148–149
Biba model, 148–149
case studies, 176–177
declassification, 156
FIPS-199 (Federal Information Processing Standard 199), 150–152
FOIA (Freedom of Information Act) and, 150
importance of, 75
life cycle of, 149
national security information, 152–154
NPPI (nonpublic personally identifiable information), 154–155
private sector information, 154
reclassification, 156
sample policy, 155
small business considerations, 163–164

information custodians, 82–83, 114, 194

information owners, 82, 114, 146–147

Information Protection Processes and Procedures category (NIST Cybersecurity Framework), 209, 589

Information Security Incident Management domain (ISO 27002 standard), 91, 369

Information Security Officers. *See* ISOs (Information Security Officers)

Information Security Policies domain (ISO 27002 standard), 87

information security policy templates (SANS), 615–616

information sharing, 278–280, 384

Information Sharing and Analysis Centers (ISACs), 279–280

information systems

acquisition, development, and maintenance. *See* SDLC (systems development life cycle)

defined, 146

inventory, 159–162

SDLC (systems development life cycle)

COTS (commercial off-the-shelf software), 342–343

development/acquisition phase, 340–341

disposal phase, 341–342

encryption, 350–355

initiation phase, 340

insecure code, 345–346

NIST Special Publications, 339

operations/maintenance phase, 341

overview, 339–340

OWASP (Open Web Application Security Project), 346–349

SAMM (Software Assurance Maturity Model), 345

sample policy, 342

secure code, 345–346

testing environment, 344

Information Systems Acquisition, Development, and Maintenance domain (ISO 27002 standard), 91, 339

Information Systems Audit and Control Association (ISACA), 114, 617

Information Systems Security Association, Inc. (ISSA), 617

Information Technology Examination Handbook (FFIEC), 474

Informative References (NIST), 586

infrastructure

access controls, 307–311

critical sectors, 2

recovery, 446

ingress traffic, 311

inherent risk, 127, 472

initiation phase (SDLC), 340

injection, 347

input validation, 347–348

insecure code, 345–346

insert skimmers, 558

insider threats, 190

Institute of Internal Auditors, 617

insurance, cyber, 125

integrated cybersecurity, 105–106

Integrated Risk Management Program, 592–593

integration, normative, 26

integrity

cryptography and, 350

data, 78

defined, 77–78

FIPS-199 (Federal Information Processing Standard 199), 151

HIPAA controls, 522

system, 78

Intel case study, 606

intellectual property (IP), 164

intentional unauthorized access, 372–373

Interagency Guidelines

Board of Directors, 469–471

defined, 468

FFIEC Cybersecurity Assessment Tool, 474–475

FFIEC IT handbook, 474

identity theft, 484–485

overview, 468–469

program adjustments, 479

reports, 479–480

risk assessment, 471–472

risk management, 473

service provider oversight, 477–478

terminology, 469

testing, 476–477

training, 476

internal audits, 113

internal product security vulnerabilities, 391–392

Internal Revenue Service (IRS), W-4 form, 186–187

Internal Security Assessors (ISAs), 565

Internal Use classification, 154, 157

International CPTED Association (ICA), 212

International Electrotechnical Commission (IEC), 85

International Information Systems Security Certification Consortium (ISC2), 617

International Mobile Equipment Identity (IMEI) numbers, 549

International Standards Organization. *See* ISO (International Standards Organization)

Internet Banking Environment Guidance, 486–487

Internet Crime Complaint Center (IC3), 487

Internet Engineering Task Force (IETF), 267–268, 318

Internet Message Access Protocol (IMAP), 262

Internet of Things (IoT), 10–11

Internet Protocol Flow Information Export (IPFIX), 267–268

Internet service providers (ISPs), 79

interviews, employee, 182

introduction, policy, 52–54

intrusion detection systems (IDSs), 314–315

intrusion prevention systems (IPSs), 314–315

inventory, 159–163

investigating incidents

documentation, 398

evidence handling, 377

forensic analysis

CCFP (Certified Cyber Forensics Professional) certification, 400

chain of custody, 223, 377, 400–401

evidence storage and retention, 401

process, 399–400

sample policy, 401–402

law enforcement, 398–399

overview, 397

Investigative phase (security clearance), 186

InvGate Assets, 162

IOCs (indicators of compromise), 268, 291–292

IoT (Internet of Things), 10–11

IP (intellectual property), 164

IP addresses, 161–162, 312

IPFIX (Internet Protocol Flow Information Export), 267–268

IPsec, 318

IPSs (intrusion prevention systems), 314–315

IRCs (incident response coordinators), 395

IRS (Internal Revenue Service), W-4 form, 186–187

IRTs (incident response teams), 113

authority, 396

CSIRTs (Cisco Computer Security Incident Response Teams), 384, 393–394

MSSPs (Managed Security Service Providers), 394

personnel, 394–396

providers, 394

PSIRTs (Product Security Incident Response Teams), 387

ISACA (Information Systems Audit and Control Association), 114, 617

ISACs (Information Sharing and Analysis Centers), 279–280

ISAs (Internal Security Assessors), 565

ISC2 (International Information Systems Security Certification Consortium), 617

(ISC)2 CCFP (Certified Cyber Forensics Professional) certification, 400

ISE (Identity Service Engine), 40

ISO (International Standards Organization)

27000 series standards. *See* 27000 series standards (ISO/IEC)

31000 series standards, 104

overview, 84–85

isolation transformers, 218

ISOs (Information Security Officers)
mobile device theft reported to, 225
responsibilities of, 147, 215
risk assessments conducted by, 213
workspace classifications, 215
ISPs (Internet service providers), 79
ISSA (Information Systems Security Association, Inc.), 617
ITL bulletins, 84

J

jargon, avoiding, 45, 47
JC Penney, data breach of, 556
JetBlue, data breach of, 556
Jha, Paras, 399
job postings, 181

K

KASLR (kernel address space layout randomization), 349
Kaspersky, 257
kernel address space layout randomization (KASLR), 349
keyloggers, 251–252
keys, 351–355
keyspace, 352
knowledge-based authentication, 299–300
Konstantinov, Kevin, 558
Krebs, Brian, 487, 558

L

labeling, 156, 303
LAPSE Project (OWASP), 346
laptops, 224–225
law enforcement, incident investigation by, 398–399
layered border security. *See* border security, layered
layered defense model, 210
leadership, effectiveness of, 24
least privilege, 297–298, 520
legislature, defined, 17
libraries, Payment Security Standards Council, 615
life cycle, systems development. *See* SDLC (systems development life cycle)
likelihood of occurrence, 128, 141
line filters, 218
local governments, role in cybersecurity policies, 19–21
location, site, 211
lockscreen ransomware, 252
logic bombs, 61, 253
logical addresses, 161–162
logs
analyzing, 271–273
identifying indicators of compromise with, 291–292
management of, 268
overview, 267–268
prioritizing and selecting, 268–271
regulatory requirements, 272
sample policy, 273
SIEM (Security Information and Event Manager), 271
Lord & Taylor, data breach of, 567
low potential impact, 150
Luhn, Hans Peter, 549
Luhn algorithm, 549–550

M

MAC (Media Access Control) addresses, 161
Mac OS X user accounts, 324
MACs (mandatory access controls), 304
magnetic strips, 549
mainframe recovery, 445
Maintenance category (NIST Cybersecurity Framework), 589

malvertising, 61

malware

APTs (advanced persistent threats), 250–251

AV (antivirus) software, 254–258

botnets, 252

bots, 252

C&C (command and control) servers, 251–252

defense-in-depth strategy, 253

defined, 250, 374

detection control, 254

downloaders, 253

email attachments with, 263–264

hybrid, 251

keyloggers, 251–252

logic bombs, 253

payment card data breaches, 555–556

prevention control, 253–254

ransomware, 252

rootkits, 252–253

sample policy, 258

screen scrapers, 251–252

spammers, 253

spyware, 253

Trojan horses, 251–252

viruses, 251

worms, 251

Managed Security Service Providers (MSSPs), 311, 394

ManageEngine AssetExplorer, 162

Massachusetts

Payment Security Standards Council, 20

Security Breach Notification Law, 407

materials, destruction of, 223

maximum tolerable downtime (MTD), 434

MBCP (Master Business Continuity Professional), 439

MBR (master boot record), overwriting, 222

McAfee case study, 606

MD5 hash function, 351

MDM (mobile device management), 224

media

HIPAA compliance, 518–520

physical security, 224–225

Media Access Control (MAC) addresses, 161

member information, 469

member information systems, 469

memory cards, 301

merchants, PCI compliance for. *See* PCI DSS (Payment Card Industry Data Security Standard)

message integrity, 351

metadata, 221, 263

Mirai botnet, 252, 373, 399

mirrored sites, 443

mitigating risk, 124

MITRE CWE (Common Weakness Enumeration), 346

mobile device management (MDM), 224

mobile sites, 442

monitoring

change, 246–247

cybersecurity policies, 26

employees, 188–189

logs

analyzing, 271–273

case study, 291–292

management of, 268

overview, 267–268

prioritizing and selecting, 268–271

regulatory requirements, 272

sample policy, 273

SIEM (Security Information and Event Manager), 271

networks, 559–560

service providers, 276

system access, 325–326

motor vehicle records, checking, 184–185

MSSPs (Managed Security Service Providers), 394

MTD (maximum tolerable downtime), 434

multi-factor authentication, 301, 303

multilayer authentication, 303

mutual authentication, 318–319

N

NAC (Network Access Control), 40, 319

NACD (National Association of Corporate Directors), 110

NACHA Corporate Account Takeover Resource Center, 487

NARA (National Archives and Records Administration), 467

Nasdaq, data breach of, 556

NAT (Network Address Translation), 313

National Council of Teachers of English, 45

National Initiative for Cybersecurity Education (NICE), 194

National Institute of Standards and Technology. *See* NIST (National Institute of Standards and Technology)

National Institute of Standards and Technology Act, 583

National Marine Fisheries Service (NMFS), plain language use by, 46

National Security Agency (NSA), degaussing standards, 222

national security information, classification of, 152–154

National Technology Transfer and Advancement Act, 583

National Telecommunications and Information Association (NTIA), 249

NCAS (National Cyber Awareness System), 370

NCCIC (National Cybersecurity and Communications Integration Center), 370

NCUA (National Credit Union Agency), 18, 466

need-to-know, 303, 520

negatives, true versus false, 373–374

NetFlow, 267–268

Network Access Control (NAC), 40, 319

Network Address Translation (NAT), 313

Network layer (OSI model), 256

network models, 256–257

network security, 10

networks

- border security, layered, 311–317
- infrastructure, 307
- monitoring, 559–560
- recovery, 446
- remote access security, 317–318
- segmentation, 308–311
- testing, 559–560

New Hampshire breach notification law, 408

New York cybersecurity regulations, 20, 70, 107, 480–482

NICE (National Initiative for Cybersecurity Education), 194, 205–206

NIS Directive, 22, 121

NIST (National Institute of Standards and Technology). *See also* NIST Cybersecurity Framework

- CSD (Computer Security Division), 83
- CyberSeek, 205–206
- NICE (National Initiative for Cybersecurity Education), 194, 205–206
- NISTIR (NIST Internal or Interagency Reports), 84
- risk assessment methodology, 130–131
- role of, 83–84
- Special Publications, 83–84, 608–613
  - access control, 89, 295
  - asset management, 88
  - business continuity, 91, 427
  - communications security, 90, 237
  - compliance management, 92
  - cryptography, 89
  - email security, 262
  - human resources, 179
  - human resources security management, 88
  - incident response, 369
  - information security incident management, 91
  - information security policies, 87
  - information systems acquisition, development, and maintenance, 91

malware, 251
NICE (National Initiative for Cybersecurity Education), 194
operations security, 90
organization of information security, 88
patch management, 249
physical and environmental security, 90, 209–210
regulatory compliance for health-care sector, 504
SDLC (systems development life cycle), 339

NIST Cybersecurity Framework
asset management, 145
business continuity, 427
communications security, 237
Cybersecurity Framework Spreadsheet project, 588, 605
defined, 83, 584
development of, 582–583
Framework Core, 585–591
Framework Profiles, 584
Framework Tiers, 584, 591–594
goals of, 582–583
governance subcategories, 118–120
human resources, 179
implementation of, 595–600
Information Assurance Framework, 83–84
Informative References, 586
Intel case study, 606
mapping HIPAA to, 526–527
McAfee case study, 606
overview, 4, 85, 583–584
physical and environmental security, 209–210
Reference Tool, 597–599
website, 608

NISTIR (NIST Internal or Interagency Reports), 84

Nixon, Richard, 45

NMFS (National Marine Fisheries Service), plain language use by, 46

non-disclosure agreements, 191

nonpublic information (NPI), 164

nonpublic personally identifiable information (NPPI), 19–20, 154–155, 164, 182, 465

nonrepudiation, 350

normalization, log, 271

normative integration, 26

North Carolina State University, Produce Safety SOP template, 242

notations, administrative, 59

NPI (nonpublic information), 164

NPPI (nonpublic personally identifiable information), 19–20, 154–155, 164, 182, 465

NSA (National Security Agency), degaussing standards, 222

NTIA (National Telecommunications and Information Association), 249

O

O2 Platform (OWASP), 346

OASIS Open Command and Control (OpenC2), 280

Obama, Barack, 152

object capability, 303

objectives, 55–56

OCC (Office of the Comptroller of the Currency), 18, 21, 466

occurrence, likelihood of, 128, 141

OCSP (Online Certificate Status Protocol), 355

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 129

OEPs (occupant emergency plans), 441

off-boarding, 180

offensive risk controls, 124

Office of the Comptroller of the Currency (OCC), 18, 21, 466

offices, physical access to, 214–215

OMB Circular A-119, 583

Omni Hotels & Resorts, data breach of, 567

Omnibus Rule, 527–528

onboarding, 179, 187

OnePlus, data breach of, 556

one-time passcode (OTP), 301

Online Certificate Status Protocol (OCSP), 355

open mail relay, 265

open security posture, 296

open source intelligence (OSINT), 279

Open System Interconnection (OSI) model, 256–257

Open Web Application Security Project. *See* OWASP (Open Web Application Security Project)

OpenC2 (OASIS Open Command and Control), 280

open-source software, 342–343

operational business functions, 441

operational change control. *See* change control

operational contingency plans, 444–445

operational management, business continuity and, 437

operational risk, 472

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 129

operations security. *See also* malware

- change control, 243–247
- collaboration services, 266
- data replication, 258–261
- email, 262–267
- logs
  - analyzing, 271–273
  - identifying indicators of compromise with, 291–292
  - management of, 268
  - overview, 267–268
  - prioritizing and selecting, 268–271
  - regulatory requirements, 272
  - sample policy, 273
  - SIEM (Security Information and Event Manager), 271
- NIST Cybersecurity Framework, 237
- overview, 236–237
- security patches, 248–250
- service provider oversight, 274–278
- SOPs (standard operating procedures)
  - defined, 238
  - developing, 239–243
  - documentation for, 238–239
  - flowcharts, 241–242
  - graphic format, 241
  - hierarchical format, 240–241
  - plain language in, 239
  - sample policy, 243
  - simple step format, 240
  - writing resources for, 242
- threat intelligence and information sharing, 278–280

Operations Security domain (ISO 27002 standard), 90, 237

operations/maintenance phase (SDLC), 341

Orbitz, data breach of, 567

Organization of Information Security domain (ISO 27002 standard), 87–88

organizational structure, 440

organizations, HIPAA compliance standards for, 524–525

orientation, employee, 180, 188–189

original classification, 153

Originator entity (syslog), 271

Orizon Project (OWASP), 346

OSI (Open System Interconnection) model, 256–257

OSINT (open source intelligence), 279

OTP (one-time passcode), 301

out-of-band authentication, 301

out-of-wallet challenge questions, 299–300

output validation, 348

Outsourcing Technology Services Handbook (FFIEC), 478

overwriting data, 222

OWASP (Open Web Application Security Project), 346–349

owners, information, 82, 114, 146–147

ownership-based authentication, 301

P

Pacific Offshore Cetacean Take Reduction Plan, plain language in, 46

packet filtering, 312–313

Palamida, 392

PANs (Primary Account Numbers), 548

Partial tier (NIST Framework), 592

partition table, overwriting, 222

passive voice, 47–48

passwords

- cognitive, 299–300
- defaults, 553
- temporary, 299
- vulnerabilities, 299
- Yahoo! password compromise, 300

PAT (Port Address Translation), 314

patches, security, 248–250, 343

pattern change evasion, 374

Paulison, David, 452

payment brands, 548

Payment Card Industry Security Standards Council , 547, 615. *See also* PCI DSS (Payment Card Industry Data Security Standard)

payroll employee data, 187

PCI DSS (Payment Card Industry Data Security Standard)

- account data elements, 548
- business-as-usual approach, 551–552
- cardholder data environments, 548
- compliance, 564–568
- core principles
  - access control, 556–558
  - cardholder data protection, 554
  - cybersecurity policies, 560
  - DESV (Designated Entities Supplemental Validation), 561
  - network monitoring and testing, 559–560
  - overview, 550–551
  - secure network and systems, 553–554
  - vulnerability management program, 555–556
- credit card elements, 549–550
- log review, 272
- Luhn algorithm, 549–550
- overview, 107, 546–547
- PANs (Primary Account Numbers), 548
- payment card data breaches, 578–579
- requirements, 552
- roles and responsibilities, 120
- terminology, 547–548
- topic summary, 561–563

PCI Forensic Investigators (PFIs), 548

PDM (Product Development Methodology), 392

penalties

- for HITECH noncompliance, 528–529
- for PCI DSS noncompliance, 567–568

perimeter networks, 308

perimeter security, 10, 212–213, 233

personal firewalls, 255

personal identification numbers (PINs), 301

PFIs (PCI Forensic Investigators), 548

pharming, 61

PHI (Personal Healthcare Information). *See* NPPI (nonpublic personally identifiable information)

phishing, 61

Physical and Environmental Security domain (ISO 27002 standard), 89–90, 209

Physical layer (OSI model), 256

physical safeguards (HIPAA), 517–520

physical security, 10

- access control, 213–216
- assessing, 231–232
- cloud and, 210–211
- data disposal, 221–223
- equipment protection, 217
- fire protection, 219–220
- layered defense model, 210
- mobile devices and media, 224–225
- NIST Cybersecurity Framework, 209–210
- NIST Special Publications, 209–210

overview, 208–209
physical access social engineering case study, 233–234
power protection, 217–219
site design, 211–213, 233
small business considerations, 225
PIE (position-independent executable), 349
PII (personally identifiable information). *See* NPPI (nonpublic personally identifiable information)
PKI (Public Key Infrastructure), 353
PLAIN (Plain Language Action and Information Network), 46–47
A Plain English Handbook (SEC), 45
plain language
active versus passive voice, 47–48
defined, 44–47
Federal Plain Language Guidelines, 46–47
jargon, avoiding, 47
jargon and, 45
National Marine Fisheries Service case study, 46
PLAIN (Plain Language Action and Information Network), 46–47
Plain Language Movement, 45–46
in SOPs (standard operating procedures), 239
U.S. Army Clarity Index, 48–49
Warren Buffet on, 45
Plain Writing Act, 46
plans
business continuity, 430
BCPs (business continuity plans), 436
disaster response plans, 440–443
operational contingency plans, 444–445
change control, 245–246
HIPAA contingency plans, 513–515
Incident Response, 44
incident response, 379–380
purpose of, 43–44
playbooks, incident response, 383–384
policies. *See also* governance; legislation
adoption of, 26
approving, 24
assets, 9–11
authorizing, 24
championing, 25
characteristics of, 13–17
components of
administrative notations, 59
definition section, 60–61
enforcement clause, 58
exceptions, 57–58
exemption process, 57–58
goals and objectives, 55–56
heading, 54–55
introduction, 52–54
sample policy, 56–57
table of, 51
terms and definitions, 60–61
version control, 51–52
corporate culture, 7–8
credit union case study, 35
defense-in-depth, 9–10
defined, 9
development of, 23–24
enforcing, 26
evaluating, 114–115
formatting, 49–51
global, 21–22
government role in. *See* regulatory requirements
guiding principles, 6–7
hierarchy of, 39
HIPAA compliance standards, 525–526
historical perspective, 5–6
implementation of, 26
importance of, 4
information security compared to, 4
items supporting, 39–44
library case study, 70
life cycle of, 22–23

maintenance of, 560
monitoring, 26
physical security
authorized entry, 213
background checks, 213–214
clear desks and screens, 216
CPTED (Crime Prevention Through Environmental Design), 212
data disposal, 221–223
equipment protection, 217
fire protection, 219–220
layered defense model, 210–211
perimeter security, 212–213
power protection, 217–219
working in secure areas, 215
workspace security, 214–215
planning, 23, 43–44
publication of, 24–25
purpose of, 105
reauthorizing, 26
researching, 23
retiring, 26
review, 26
templates, 70
vetting, 24
writing, 24
case study, 101
plain language, 44–49

policy pie, 11–17

polyalphabetic ciphers, 350

POP3 (Post Office Protocol 3), 262

Port Address Translation (PAT), 314

portals, remote access, 318

ports, 312

position-independent executable (PIE), 349

positive validation, 347–348

positives, true versus false, 373–374

possession-based authentication, 301

Post Office Protocol 3 (POP3), 262

post-implementation, 26

post-incident activity, 383

post-mortems, 383

power protection, 217–219

power spikes, 217

power surges, 217

preparation phase (incident response), 381

Presentation layer (OSI model), 256

presidential directives and orders
Critical Infrastructure Security and
Resilience, 3
Directive-63 (PDD-63), 279
Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 4
Protecting Critical Infrastructure, 3

pretexting (GLBA), 465

prevention control, 253–254

Primary Account Numbers (PANs), 548

principle of least privilege, 297–298

principles, guiding, 6–7

prioritizing log data, 268–271

privacy, 184, 188–189

Privacy Officers, 113

Privacy Rule (GLBA), 465

private keys, 353

private sector information, classification of, 154

procedures, defined, 42–43

Produce Safety SOP template, 242

Product Development Methodology (PDM), 392

Product Security Incident Response Teams (PSIRTs), 387

product security vulnerabilities
chaining, 391
internal versus external, 391–392
severity levels, 387–390
theoretical, 391

professional development programs, 617

profiles, NIST Cybersecurity Framework, 584

programs, defined, 43–44

Protecode, 392

Protect function (NIST Framework Core), 588–589

Protected classification, 154, 157

Protective Technology category (NIST Cybersecurity Framework), 589

protocols, defined, 312

providers, incident response, 394

province governments, role in cybersecurity policies, 19–21

proxying, 374

PSIRTs (Product Security Incident Response Teams), 387

Public Doublespeak Committee, 45

Public information, 154

Public Key Infrastructure (PKI), 353

public keys, 353

public relations, data breaches and, 409–410

public trust, honoring, 8, 34

purple teaming, 316

Q

QSAs (Qualified Security Assessors), 548, 565

Qualys, 297

R

ransomware, 252

Rapid7 Nexpose, 297

RAs (Registration Authorities), 353

ratings, examination, 483–484

RBACs (role-based access controls), 304

RCs (release candidates), 343

Reagan, Ronald, 45

realistic policies, 13–14

reauthorizing policies, 26

reciprocal sites, 443

reclassification of information, 156

Recover function (NIST Framework Core), 590

recovery, disaster

- overview, 445–446
- plans, 436, 445
- procedures, 446–447
- RPO (recovery point objective), 258, 434
- RTO (recovery time objective), 258, 434
- sample policy, 448
- service provider dependencies, 447

recruitment

- candidate data, 182
- defined, 179
- employee screening, 183–186
- government clearance, 186
- interviews, 182
- job postings, 181
- sample policy, 182

red teams, 316

reducing risk, 124

Reference Tool (NIST Cybersecurity Framework)

- Home screen, 597
- overview, 597–599
- searching with, 599
- views, 597–598

reflected DDoS (distributed denial-of-service) attacks, 80

Registration Authorities (RAs), 353

Relay entity (syslog), 271

release candidates (RCs), 343

releases, software, 343

relevant policies, 13

relocation strategies, 441–443

remote access security, 224, 317–321

removing assets, 162

Repeatable tier (NIST Framework), 593

replication, data, 258–261

reports

- audit, 114
- incident response, 376–378
- Interagency Guidelines, 479–480
- ROCs (Reports on Compliance), 565–566
- SIEM (Security Information and Event Manager), 271

reputational risk, 472

Requests for Change. *See* RFCs (Requests for Change)

Requests for Information (RFIs), 600

required implementations, 507

researching policies, 23

residual risk, 128, 472

resilience, 428–429

resources, cybersecurity

- HIPAA Security Series, 609–613
- information security professional development and certification programs, 617
- NIST Cybersecurity Framework, 608
- NIST Special Publications, 608–613
- Payment Security Standards Council, 615

Respond function (NIST Framework Core), 590

response plans, 436

resumption phase, 436, 448

retaining evidence, 401

retiring policies, 26

reviewing policies, 26

revising policies, 117

RFCs (Requests for Change), 244–245

RFIs (Requests for Information), 600

risk

- acceptance of, 124
- advantages of, 123
- appetite for, 126
- assessment of
  - case study, 141
  - controls, 128
  - FAIR (Factor Analysis of Information Risk), 129–130
  - impact, 128
  - inherent risk, 127
  - likelihood of occurrence, 128, 141
  - NIST methodology, 130–131
  - OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 129
  - overview, 127–128
  - residual risk, 128
  - threat sources, 127
  - threats, 127
  - vulnerabilities, 128
- avoidance of, 124
- business continuity, 430–436
- compliance, 472
- cyber insurance, 125
- defined, 122–123
- HIPAA (Health Insurance Portability and Accountability Act), 508–509
- inherent, 472
- Interagency Guidelines
  - FFIEC Cybersecurity Assessment Tool, 474–475
  - FFIEC IT handbook, 474
  - program adjustments, 479
  - reports, 479–480
  - risk assessment, 471–472
  - risk management, 473
  - service provider oversight, 477–478
  - testing, 476–477
  - training, 476
- management process (NIST), 592–593
- mitigation of, 124
- operational, 472
- oversight policy, 127
- reduction of, 124
- reputational, 472
- residual, 472
- response policy, 125
- sharing, 124
- small business considerations, 126
- strategic, 472
- tolerance of, 123, 126
- transactional, 472
- transferring, 124

Risk Assessment category (NIST Cybersecurity Framework), 587

Risk Informed tier (NIST Framework), 592

ROCs (Reports on Compliance), 565–566

role-based access controls (RBACs), 304, 511

roles, business continuity, 437–439

rollback strategy, 343

rooms, physical access to, 214–215

rootkits, 252–253

RPO (recovery point objective), 258, 434

RTO (recovery time objective), 258, 434

rule-based access controls, 305

runtime defenses, 349

S

safe harbor provision (HITECH), 530

Safeguards Rule (GLBA), 465, 467–468

sags, power, 217

Saks Fifth Avenue, data breach of, 567

SAMM (Software Assurance Maturity Model), 345

SANS Institute, 615–617

Sapphire, 251

SAQ (PCI DSS Self-Assessment Questionnaire), 566–567

SAR (Suspicious Activity Report) regulations, 404

Sarbanes-Oxley (SOX), 107

SAST (Static Application Security Testing) tools, 346

SBA (Small Business Administration), 452

SBU (Sensitive But Unclassified) information, 152, 153

SC (security category), 150

schemes, identification, 295

screen scrapers, 251–252

screening employees, 183–186

screens, clear, 216

scrubbing, 222

SDL (secure development life cycle), 391

SDLC (systems development life cycle), 338

- COTS (commercial off-the-shelf software), 342–343
- development/acquisition phase, 340–341
- disposal phase, 341–342
- encryption
  - advantages of, 351–352
  - CAs (Certification Authorities), 353
  - cipher text, 350
  - cryptography, 350
  - decryption, 351
  - defined, 350–351
  - digital certificates, 353–355
  - digital signatures, 351
  - hashing, 351
  - keys, 351–355
  - message integrity, 351
  - PKI (Public Key Infrastructure), 353
  - RAs (Registration Authorities), 353
  - regulatory requirements, 352
  - small business considerations, 356
- initiation phase, 340
- insecure code, 345–346
- NIST Special Publications, 339
- operations/maintenance phase, 341
- overview, 339–340
- OWASP (Open Web Application Security Project), 346–349
- SAMM (Software Assurance Maturity Model), 345
- sample policy, 342
- secure code, 345–346
- testing environment, 344

searching, NIST CSF Reference Tool, 599

SEC (Securities and Exchange Commission), 45, 466

Secret (S) information, 153

Secret Service, 398–399, 487

secure code, 345–346

secure development life cycle (SDL), 391

secure security posture, 296

security awareness, 194, 250, 511–512

security category (SC), 150

Security Continuous Monitoring category (NIST Cybersecurity Framework), 209

security domains, 73

Security Education, Training, and Awareness. *See* SETA (Security Education, Training, and Awareness) model

security framework. *See* NIST Cybersecurity Framework

security incident procedures (HIPAA), 512–513

Security Information and Event Manager (SIEM), 271

security labels, 303

security management process (HIPAA), 508–509

security patches. *See* patches, security

SEDs (Self-Encrypting Drives), 222

segmentation, network, 308–311

segregation of duties, 323

SEI (Software Engineering Institute), 393

Self-Assessment Questionnaire (PCI DSS), 566–567

Self-Encrypting Drives (SEDs), 222

semi-trusted networks, 308

sensitive areas, 557

Sensitive But Unclassified (SBU) information, 152, 153

sensitive personal information (SPI). *See* NPPI (nonpublic personally identifiable information)

servers

- C&C (command and control), 251–252
- email, 265

service level agreements (SLAs), 79

service provider oversight

- audits of, 275
- contracts, 275–276
- dependencies, 447
- due diligence, 274–275
- Interagency Guidelines, 477–478
- monitoring, 276
- overview, 274
- sample policy, 277
- service provider definition, 469, 548
- small business considerations, 278
- strengthening resilience of, 274

ServiceNOW, 162

Session layer (OSI model), 256

session management, 349

SETA (Security Education, Training, and Awareness) model

- defined, 194
- importance of, 193–194
- overview, 186–187
- sample policy, 195
- security awareness, 194

severity levels

- incidents, 375–376
- product security vulnerabilities, 387–390

SHA hash function, 351

shoulder surfing, 216

SIEM (Security Information and Event Manager), 271

signatures, digital, 351

silo-based cybersecurity, 105–106

Simple Mail Transfer Protocol (SMTP), 262

simple step format (SOPs), 240

simulations, tabletop, 449

single-factor authentication, 303

singular policies, 49–51

sites, physical security for, 211–213, 233

skimmers, 558

Slack, 266

Slammer, 251

SLAs (service level agreements), 79

small businesses

- access control, 326
- digital certificates, 356
- disaster response plans, 452
- human resources in, 195
- information classification in, 163–164
- physical security issues specific to, 225
- risk management in, 126
- SBA (Small Business Administration), 452
- service providers and, 278

smartcards, 301

SMTP (Simple Mail Transfer Protocol), 262

social media
  disaster response and, 460
  screening employees through, 184
software assets, inventory of, 160
Software Assurance Maturity Model (SAMM), 345
Software Engineering Institute (SEI), 393
software keys, 162
SolarWinds Web Help Desk, 162
soliciting feedback, 26
SonarQube Project (OWASP), 346
SOPs (standard operating procedures), 238–243
SOX (Sarbanes-Oxley), 107
SP. *See* Special Publications (NIST)
spammers, 253
Special Publications (NIST), 83–84, 608–613
  access control, 89, 295
  asset management, 88
  business continuity, 91, 427
  communications security, 90, 237
  compliance management, 92
  cryptography, 89
  email security, 262
  human resources, 179
  human resources security management, 88
  incident response, 369
  information security, 87
  information security incident management, 91
  information security policies, 87
  information systems acquisition, development, and maintenance, 91
  malware, 251
  NICE (National Initiative for Cybersecurity Education), 194
  operations security, 90
  organization of information security, 88
  patch management, 249
  physical and environmental security, 90, 209–210
  regulatory compliance for health-care sector, 504
  SDLC (systems development life cycle), 339
SPI (sensitive personal information). *See* NPPI (nonpublic personally identifiable information)
spikes, power, 217
spoofing, 374
spreadsheets, Cybersecurity Framework, 588, 605
SpyEye, 251–252
spyware, 253
SSAE18 audit reports, 275
stakeholders, communication with, 595–596
standard operating procedures. *See* SOPs (standard operating procedures)
Standards for Attestation Engagements (SSAE), 275
state governments, role in cybersecurity policies, 19–21, 529
statements, policy, 56–57
Static Application Security Testing (SAST) tools, 346
STIX (Structured Threat Information Expression), 280
storing evidence, 401
strategic alignment, 105–107
strategic risk, 472
structured review, 449
Structured Threat Information Expression (STIX), 280
student records, privacy of, 19
su command, 324
subcontractors, HITECH compliance standards, 528
subjects, 295
submitting RFCs (Requests for Change), 245
substitution ciphers, 350
successful access, 325
sudo command, 324

Supplier Relationship domain (ISO 27002 standard), 91

supply chain attacks, 257

supply chain relationships, 595–596

Supply Chain Risk Management category (NIST Cybersecurity Framework), 587

surge protection, 217, 218

Suspicious Activity Report (SAR) regulations, 404

symmetric keys, 352–353

Synopsys BlackDuck, 392

Synopsys Protecode, 392

syslog, 270–271

system components, 548

system integrity, 78

systems development life cycle. *See* SDLC (systems development life cycle)

T

tabletop exercises, 383–384, 449

tablets, 224–225

tailgating, 213

Target Corp., data breach of, 556

TAXII (Trusted Automated Exchange of Indicator Information), 280

TC-NAC (Threat-Centric Network Access Control), 297

TCP/IP (Transmission Control Protocol/ Internet Protocol) model, 256–257

teams, incident response

- authority, 396
- CSIRTs (Cisco Computer Security Incident Response Teams), 384, 393–394
- defined, 113
- MSSPs (Managed Security Service Providers), 394
- personnel, 394–396
- providers, 394
- PSIRTs (Product Security Incident Response Teams), 387

technical safeguards (HIPAA), 520–525

technology service providers (TSPs), 478

TelCoa (Telework Coalition), 320

Telepresence, 266

Telework Coalition (TelCoa), 320

Telework Enhancement Act, 320

teleworking access controls, 320–321

templates

- policy, 70
- SANS information security policy, 615–616

temporary files, 221

temporary passwords, 299

Tenable Security Center, 297

termination, employee, 180, 189–190

testing

- business continuity, 449–450
- data replication, 261
- environment for, 344
- Interagency Guidelines, 476–477
- networks, 559–560

Texas Breach Notification Law, 407

theoretical product security vulnerabilities, 391

third-party service provider relationships, 477

third-party software (TPS) security, 391–392

threat intelligence and information sharing, 278–280

Threat-Centric Network Access Control (TC-NAC), 297

threats. *See also* attacks; malware

- blended, 255
- business continuity, 430–431
- defined, 127
- insider, 190
- intelligence and information sharing, 278–280

tiers, NIST Framework, 584, 591–594

- Adaptive (Tier 4), 593–594
- Partial (Tier 1), 592
- Repeatable (Tier 3), 593
- Risk Informed (Tier 2), 592

TLS (Transport Layer Security), 75

tolerance, risk, 123

Tomlinson, Ray, 261–262

Top Secret (TS) information, 152–153

Torah, as policy, 583–584

TPS (third-party software) security, 391–392

training, 25

business continuity management, 439

defined, 194

DHHS HIPAA training, 529

HIPAA (Health Insurance Portability and Accountability Act), 511–512

importance of, 193–194

incident response, 396

Interagency Guidelines, 476

professional development programs, 617

sample policy, 195

security awareness, 194

transactional risk, 472

transferring risk, 124

Transmission Control Protocol/Internet Protocol (TCP/IP) model, 256–257

transmission security, HIPAA, 523

Transport layer (OSI model), 256

Transport Layer Security (TLS), 75

transposition ciphers, 350

Trojan horses, 61, 251–252

Trump, Donald, 4

Trump Hotels, data breach of, 567

trust, public, 8, 34

Trusted Automated Exchange of Indicator Information (TAXII), 280

trusted networks, 308

TS (Top Secret) information, 152–153

TSPs (technology service providers), 478

Tyco, 183

U

Unclassified (U) information, 153

Uniform Rating System for Information Technology (URSIT), 483–484

uninterruptible power supplies (UPSs), 218

unique identifiers, 160–161

The Untouchables, 77–78

untrusted networks, 308

updates, software, 343

UPSs (uninterruptible power supplies), 218

URSIT (Uniform Rating System for Information Technology), 483–484

US-CERT (United States Computer Emergency Readiness Team), 370, 393

user access controls, 321–324

user provisioning, 179, 187–188

user-level cybersecurity policies, 108

V

validation, 448, 563–564

VCDB (VERIS Community Database), 403

vendor oversight. *See* service provider oversight

vendor policies, 108

version control, 51–52

Veterans Administration, data breach notifications, 406

vetting policies, 24

views, NIST CSF Reference Tool, 597–598

virtual private networks (VPNs), 75, 318

viruses, 251

Visa compliance validation, 563–564

visitor credentialing, 213

voice, active versus passive, 47–48

voltage regulators, 218

VPNs (virtual private networks), 75, 318

vulnerabilities

CVSS (Common Vulnerability Scoring System), 387–390

defined, 128

disclosure policies, 108

product security, 387–392

vulnerability management program, 555–556

W

W-4 Form, 186–187

W32/SQL Slammer, 251

waiver process, 57–58

WannaCry, 251, 252

WAP-Web Application Protection (OWASP), 346

war rooms, 440–441

warm sites, 442

web caches, 221

WebEx, 266

Wendy's, data breach of, 556

White, Josiah, 399

white box assurance tests, 477

whitelisting, 315, 347–348

Whole Foods, data breach of, 567

Windows

Group Policy configuration, 40

user account controls, 323–324

Wofford, Cynthia, 558

Workers' Compensation history, checking, 185

workforce security (HIPAA), 510

workspaces, 214–215

workstations, HIPAA compliance, 518

worms, 251

X-Y-Z

Yahoo! password compromise, 300

zero-day exploits, 263

Zeus, 251–252