PEARSON IT CYBERSECURITY CURRICULUM

DEVELOPING CYBERSECURITY PROGRAMS AND POLICIES

OMAR SANTOS

Developing Cybersecurity Programs and Policies

Omar Santos

Pearson

Developing Cybersecurity Programs and Policies

Table of Contents

Cover
Title Page
Copyright Page
About the Author
Contents
Chapter 1: Understanding Cybersecurity Policy and Governance
Information Security vs. Cybersecurity Policies
Looking at Policy Through the Ages
Policy in Ancient Times
The United States Constitution as a Policy Revolution
Policy Today
Cybersecurity Policy
What Are Assets?
Successful Policy Characteristics
What Is the Role of Government?
Additional Federal Banking Regulations
Government Cybersecurity Regulations in Other Countries
The Challenges of Global Policies
Cybersecurity Policy Life Cycle
Policy Development
Policy Publication

Table of Contents

Policy Adoption

Policy Review

Summary

Chapter 2: Cybersecurity Policy Organization, Format, and Styles

Policy Hierarchy

Standards

Baselines

Guidelines

Procedures

Plans and Programs

Writing Style and Technique

Using Plain Language

The Plain Language Movement

Plain Language Techniques for Policy Writing

Policy Format

Understand Your Audience

Policy Format Types

Policy Components

Summary

Chapter 3: Cybersecurity Framework

Confidentiality, Integrity, and Availability

What Is Confidentiality?

What Is Integrity?

What Is Availability?

Who Is Responsible for CIA?

NISTs Cybersecurity Framework

What Is NISTs Function?

Table of Contents

So, What About ISO?
NIST Cybersecurity Framework
ISO Standards
Summary
Chapter 4: Governance and Risk Management
Understanding Cybersecurity Policies
What Is Governance?
What Is Meant by Strategic Alignment?
Regulatory Requirements
User-Level Cybersecurity Policies
Vendor Cybersecurity Policies
Cybersecurity Vulnerability Disclosure Policies
Client Synopsis of Cybersecurity Policies
Who Authorizes Cybersecurity Policy?
What Is a Distributed Governance Model?
Evaluating Cybersecurity Policies
Revising Cybersecurity Policies: Change Drivers
NIST Cybersecurity Framework Governance Subcategories and Informative References
Regulatory Requirements
Cybersecurity Risk
Is Risk Bad?
Understanding Risk Management
Risk Appetite and Tolerance
What Is a Risk Assessment?
Risk Assessment Methodologies
Summary
Chapter 5: Asset Management and Data Loss Prevention
Information Assets and Systems

Table of Contents

Who Is Responsible for Information Assets?

Information Classification

How Does the Federal Government Classify Data?

Why Is National Security Information Classified Differently?

Who Decides How National Security Data Is Classified?

How Does the Private Sector Classify Data?

Can Information Be Reclassified or Even Declassified?

Labeling and Handling Standards

Why Label?

Why Handling Standards?

Information Systems Inventory

Why an Inventory Is Necessary and What Should Be Inventoried

Understanding Data Loss Prevention Technologies

Summary

Chapter 6: Human Resources Security

The Employee Life Cycle

What Does Recruitment Have to Do with Security?

What Happens in the Onboarding Phase?

What Is User Provisioning?

What Should an Employee Learn During Orientation?

Why Is Termination Considered the Most Dangerous Phase?

The Importance of Employee Agreements

What Are Confidentiality or Nondisclosure Agreements?

What Is an Acceptable Use Agreement?

The Importance of Security Education and Training

Influencing Behavior with Security Awareness

Teaching a Skill with Security Training

Security Education Is Knowledge Driven

Summary

Table of Contents

Chapter 7: Physical and Environmental Security

- Understanding the Secure Facility Layered Defense Model
  - How Do We Secure the Site?
  - How Is Physical Access Controlled?
- Protecting Equipment
  - No Power, No Processing?
  - How Dangerous Is Fire?
  - What About Disposal?
  - Stop, Thief!
- Summary

Chapter 8: Communications and Operations Security

- Standard Operating Procedures
  - Why Document SOPs?
  - Developing SOPs
- Operational Change Control
  - Why Manage Change?
  - Why Is Patching Handled Differently?
- Malware Protection
  - Are There Different Types of Malware?
  - How Is Malware Controlled?
  - What Is Antivirus Software?
- Data Replication
  - Is There a Recommended Backup or Replication Strategy?
- Secure Messaging
  - What Makes Email a Security Risk?
  - Are Email Servers at Risk?
  - Other Collaboration and Communication Tools
- Activity Monitoring and Log Analysis

Table of Contents

What Is Log Management?

Service Provider Oversight

What Is Due Diligence?

What Should Be Included in Service Provider Contracts?

Threat Intelligence and Information Sharing

How Good Is Cyber Threat Intelligence if It Cannot Be Shared?

Summary

Chapter 9: Access Control Management

Access Control Fundamentals

What Is a Security Posture?

How Is Identity Verified?

What Is Authorization?

Accounting

Infrastructure Access Controls

Why Segment a Network?

What Is Layered Border Security?

Remote Access Security

User Access Controls

Why Manage User Access?

What Types of Access Should Be Monitored?

Summary

Chapter 10: Information Systems Acquisition, Development, and Maintenance

System Security Requirements

What Is SDLC?

What About Commercially Available or Open Source Software?

The Testing Environment

Protecting Test Data

Table of Contents

Secure Code

The Open Web Application Security Project (OWASP)

Cryptography

Why Encrypt?

Regulatory Requirements

What Is a Key?

What Is PKI?

Why Protect Cryptographic Keys?

Digital Certificate Compromise

Summary

Chapter 11: Cybersecurity Incident Response

Incident Response

What Is an Incident?

How Are Incidents Reported?

What Is an Incident Response Program?

The Incident Response Process

Tabletop Exercises and Playbooks

Information Sharing and Coordination

Computer Security Incident Response Teams

Product Security Incident Response Teams (PSIRTs)

Incident Response Training and Exercises

What Happened? Investigation and Evidence Handling

Documenting Incidents

Working with Law Enforcement

Understanding Forensic Analysis

Data Breach Notification Requirements

Is There a Federal Breach Notification Law?

Does Notification Work?

Summary

Table of Contents

Chapter 12: Business Continuity Management

Emergency Preparedness

What Is a Resilient Organization?

Regulatory Requirements

Business Continuity Risk Management

What Is a Business Continuity Threat Assessment?

What Is a Business Continuity Risk Assessment?

What Is a Business Impact Assessment?

The Business Continuity Plan

Roles and Responsibilities

Disaster Response Plans

Operational Contingency Plans

The Disaster Recovery Phase

The Resumption Phase

Plan Testing and Maintenance

Why Is Testing Important?

Plan Maintenance

Summary

Chapter 13: Regulatory Compliance for Financial Institutions

The Gramm-Leach-Bliley Act

What Is a Financial Institution?

Regulatory Oversight

What Are the Interagency Guidelines?

New Yorks Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500)

What Is a Regulatory Examination?

Examination Process

Examination Ratings

Table of Contents

Personal and Corporate Identity Theft

What Is Required by the Interagency Guidelines Supplement A?

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

Summary

Chapter 14: Regulatory Compliance for the Health-Care Sector

The HIPAA Security Rule

What Is the Objective of the HIPAA Security Rule?

How Is the HIPAA Security Rule Organized?

What Are the Physical Safeguards?

What Are the Technical Safeguards?

What Are the Organizational Requirements?

What Are the Policies and Procedures Standards?

The HIPAA Security Rule Mapping to NIST Cybersecurity Framework

The HITECH Act and the Omnibus Rule

What Changed for Business Associates?

What Are the Breach Notification Requirements?

Understanding the HIPAA Compliance Enforcement Process

Summary

Chapter 15: PCI Compliance for Merchants

Protecting Cardholder Data

What Is the PAN?

The Luhn Algorithm

What Is the PCI DDS Framework?

Business-as-Usual Approach

What Are the PCI Requirements?

PCI Compliance

Who Is Required to Comply with PCI DSS?

Table of Contents

What Is a Data Security Compliance Assessment?

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

Are There Penalties for Noncompliance?

Summary

Chapter 16: NIST Cybersecurity Framework

Introducing the NIST Cybersecurity Framework Components

The Framework Core

Identify

Protect

Detect

Respond

Recover

Framework Implementation Tiers (Tiers)

Who Should Coordinate the Framework Implementation?

NISTs Recommended Steps to Establish or Improve a Cybersecurity Program

Communication with Stakeholders and Supply Chain Relationships

NISTs Cybersecurity Framework Reference Tool

Adopting the NIST Cybersecurity Framework in Real Life

Summary

Appendix A: Cybersecurity Program Resources

Appendix B: Answers to the Multiple Choice Questions

Index

Pearson