Effective Cybersecurity
Effective Cybersecurity: A Guide to Using Best Practices and Standards

Table of Contents

Cover
Half Title
Title Page
Copyright Page
Dedication
Contents
Preface
Chapter 1: Best Practices, Standards, and a Plan of Action
  1.1 Defining Cyberspace and Cybersecurity
  1.2 The Value of Standards and Best Practices Documents
  1.3 The Standard of Good Practice for Information Security
  1.4 The ISO/IEC 27000 Suite of Information Security Standards
     ISO 27001
     ISO 27002
  1.5 Mapping the ISO 27000 Series to the ISF SGP
  1.6 NIST Cybersecurity Framework and Security Documents
     NIST Cybersecurity Framework
     NIST Security Documents
  1.7 The CIS Critical Security Controls for Effective Cyber Defense
  1.8 COBIT 5 for Information Security
  1.9 Payment Card Industry Data Security Standard (PCI DSS)
Table of Contents

1.10 ITU-T Security Documents
1.11 Effective Cybersecurity
   The Cybersecurity Management Process
   Using Best Practices and Standards Documents
1.12 Key Terms and Review Questions
   Key Terms
   Review Questions
1.13 References

Part I: Planning for Cybersecurity
Chapter 2: Security Governance
   2.1 Security Governance and Security Management
   2.2 Security Governance Principles and Desired Outcomes
       Principles
       Desired Outcomes
   2.3 Security Governance Components
       Strategic Planning
       Organizational Structure
       Roles and Responsibilities
       Integration with Enterprise Architecture
       Policies and Guidance
   2.4 Security Governance Approach
       Security Governance Framework
       Security Direction
       Responsible, Accountable, Consulted, and Informed (RACI) Charts
   2.5 Security Governance Evaluation
   2.6 Security Governance Best Practices
   2.7 Key Terms and Review Questions
       Key Terms
       Review Questions
   2.8 References
Table of Contents

Chapter 3: Information Risk Assessment

3.1 Risk Assessment Concepts
   - Risk Assessment Challenges
   - Risk Management
   - Structure of This Chapter

3.2 Asset Identification
   - Hardware Assets
   - Software Assets
   - Information Assets
   - Business Assets
   - Asset Register

3.3 Threat Identification
   - The STRIDE Threat Model
   - Threat Types
   - Sources of Information

3.4 Control Identification

3.5 Vulnerability Identification
   - Vulnerability Categories
   - National Vulnerability Database and Common Vulnerability Scoring System

3.6 Risk Assessment Approaches
   - Quantitative Versus Qualitative Risk Assessment
   - Simple Risk Analysis Worksheet
   - Factor Analysis of Information Risk

3.7 Likelihood Assessment
   - Estimating Threat Event Frequency
   - Estimating Vulnerability
   - Loss Event Frequency

3.8 Impact Assessment
   - Estimating the Primary Loss
   - Estimating the Secondary Loss
   - Business Impact Reference Table

3.9 Risk Determination
# Table of Contents

3.10 Risk Evaluation
3.11 Risk Treatment
   - Risk Reduction
   - Risk Retention
   - Risk Avoidance
   - Risk Transfer
3.12 Risk Assessment Best Practices
3.13 Key Terms and Review Questions
   - Key Terms
   - Review Questions
3.14 References

## Chapter 4: Security Management

4.1 The Security Management Function
   - Security Planning
   - Capital Planning
4.2 Security Policy
   - Security Policy Categories
   - Security Policy Document Content
   - Management Guidelines for Security Policies
   - Monitoring the Policy
4.3 Acceptable Use Policy
4.4 Security Management Best Practices
4.5 Key Terms and Review Questions
   - Key Terms
   - Review Questions
4.6 References

## PART II: Managing the Cybersecurity Function

## Chapter 5: People Management

5.1 Human Resource Security
   - Security in the Hiring Process
   - During Employment
# Table of Contents

Termination of Employment

5.2 Security Awareness and Education
   Security Awareness
   Cybersecurity Essentials Program
   Role-Based Training
   Education and Certification

5.3 People Management Best Practices

5.4 Key Terms and Review Questions
   Key Terms
   Review Questions

5.5 References

Chapter 6: Information Management

6.1 Information Classification and Handling
   Information Classification
   Information Labeling
   Information Handling

6.2 Privacy
   Privacy Threats
   Privacy Principles and Policies
   Privacy Controls

6.3 Document and Records Management
   Document Management
   Records Management

6.4 Sensitive Physical Information

6.5 Information Management Best Practices

6.6 Key Terms and Review Questions
   Key Terms
   Review Questions

6.7 References

Chapter 7: Physical Asset Management

7.1 Hardware Life Cycle Management
Table of Contents

Planning
Acquisition
Deployment
Management
Disposition

7.2 Office Equipment
  Threats and Vulnerabilities
  Security Controls
  Equipment Disposal

7.3 Industrial Control Systems
  Differences Between IT Systems and Industrial Control Systems
  ICS Security

7.4 Mobile Device Security
  Mobile Device Technology
  Mobile Ecosystem
  Vulnerabilities
  Mobile Device Security Strategy
  Resources for Mobile Device Security

7.5 Physical Asset Management Best Practices

7.6 Key Terms and Review Questions
  Key Terms
  Review Questions

7.7 References

Chapter 8: System Development

8.1 System Development Life Cycle
  NIST SDLC Model
  The SGPs SDLC Model
  DevOps

8.2 Incorporating Security into the SDLC
  Initiation Phase
  Development/Acquisition Phase
  Implementation/Assessment Phase
# Table of Contents

Operations and Maintenance Phase  
Disposal Phase  

8.3 System Development Management  
- System Development Methodology  
- System Development Environments  
- Quality Assurance  

8.4 System Development Best Practices  

8.5 Key Terms and Review Questions  
- Key Terms  
- Review Questions  

8.6 References  

# Chapter 9: Business Application Management  
9.1 Application Management Concepts  
- Application Life Cycle Management  
- Application Portfolio Management  
- Application Performance Management  

9.2 Corporate Business Application Security  
- Business Application Register  
- Business Application Protection  
- Browser-Based Application Protection  

9.3 End User-Developed Applications (EUDAs)  
- Benefits of EUDAs  
- Risks of EUDAs  
- EUDA Security Framework  

9.4 Business Application Management Best Practices  

9.5 Key Terms and Review Questions  
- Key Terms  
- Review Questions  

9.6 References  

# Chapter 10: System Access  
10.1 System Access Concepts
# Table of Contents

Authorization

## 10.2 User Authentication
- A Model for Electronic User Authentication
- Means of Authentication
- Multifactor Authentication

## 10.3 Password-Based Authentication
- The Vulnerability of Passwords
- The Use of Hashed Passwords
- Password Cracking of User-Chosen Passwords
- Password File Access Control
- Password Selection

## 10.4 Possession-Based Authentication
- Memory Cards
- Smart Cards
- Electronic Identity Cards
- One-Time Password Device
- Threats to Possession-Based Authentication
- Security Controls for Possession-Based Authentication

## 10.5 Biometric Authentication
- Criteria for Biometric Characteristics
- Physical Characteristics Used in Biometric Applications
- Operation of a Biometric Authentication System
- Biometric Accuracy
- Threats to Biometric Authentication
- Security Controls for Biometric Authentication

## 10.6 Risk Assessment for User Authentication
- Authenticator Assurance Levels
- Selecting an AAL
- Choosing an Authentication Method

## 10.7 Access Control
- Subjects, Objects, and Access Rights
- Access Control Policies
- Discretionary Access Control
Table of Contents

Role-Based Access Control
Attribute-Based Access Control
Access Control Metrics
10.8 Customer Access
   Customer Access Arrangements
   Customer Contracts
   Customer Connections
   Protecting Customer Data
10.9 System Access Best Practices
10.10 Key Terms and Review Questions
   Key Terms
   Review Questions
10.11 References

Chapter 11: System Management
11.1 Server Configuration
   Threats to Servers
   Requirements for Server Security
11.2 Virtual Servers
   Virtualization Alternatives
   Virtualization Security Issues
   Securing Virtualization Systems
11.3 Network Storage Systems
11.4 Service Level Agreements
   Network Providers
   Computer Security Incident Response Team
   Cloud Service Providers
11.5 Performance and Capacity Management
11.6 Backup
11.7 Change Management
11.8 System Management Best Practices
11.9 Key Terms and Review Questions
Table of Contents

Key Terms
Review Questions
11.10 References

Chapter 12: Networks and Communications

12.1 Network Management Concepts
   Network Management Functions
   Network Management Systems
   Network Management Architecture

12.2 Firewalls
   Firewall Characteristics
   Types of Firewalls
   Next-Generation Firewalls
   DMZ Networks
   The Modern IT Perimeter

12.3 Virtual Private Networks and IP Security
   Virtual Private Networks
   IPsec
   Firewall-Based VPNs

12.4 Security Considerations for Network Management
   Network Device Configuration
   Physical Network Management
   Wireless Access
   External Network Connections
   Firewalls
   Remote Maintenance

12.5 Electronic Communications
   Email
   Instant Messaging
   Voice over IP (VoIP) Networks
   Telephony and Conferencing

12.6 Networks and Communications Best Practices

12.7 Key Terms and Review Questions
Table of Contents

Key Terms
Review Questions
12.8 References

Chapter 13: Supply Chain Management and Cloud Security

13.1 Supply Chain Management Concepts
   The Supply Chain
   Supply Chain Management

13.2 Supply Chain Risk Management
   Supply Chain Threats
   Supply Chain Vulnerabilities
   Supply Chain Security Controls
   SCRM Best Practices

13.3 Cloud Computing
   Cloud Computing Elements
   Cloud Computing Reference Architecture

13.4 Cloud Security
   Security Considerations for Cloud Computing
   Threats for Cloud Service Users
   Risk Evaluation
   Best Practices
   Cloud Service Agreement

13.5 Supply Chain Best Practices

13.6 Key Terms and Review Questions
   Key Terms
   Review Questions

13.7 References

Chapter 14: Technical Security Management

14.1 Security Architecture

14.2 Malware Protection Activities
   Types of Malware
   The Nature of the Malware Threat
   Practical Malware Protection
Table of Contents

14.3 Malware Protection Software
   Capabilities of Malware Protection Software
   Managing Malware Protection Software

14.4 Identity and Access Management
   IAM Architecture
   Federated Identity Management
   IAM Planning
   IAM Best Practices

14.5 Intrusion Detection
   Basic Principles
   Approaches to Intrusion Detection
   Host-Based Intrusion Detection Techniques
   Network-Based Intrusion Detection Systems
   IDS Best Practices

14.6 Data Loss Prevention
   Data Classification and Identification
   Data States

14.7 Digital Rights Management
   DRM Structure and Components
   DRM Best Practices

14.8 Cryptographic Solutions
   Uses of Cryptography
   Cryptographic Algorithms
   Selection of Cryptographic Algorithms and Lengths
   Cryptography Implementation Considerations

14.9 Cryptographic Key Management
   Key Types
   Cryptoperiod
   Key Life Cycle

14.10 Public Key Infrastructure
   Public Key Certificates
   PKI Architecture
Table of Contents

Management Issues
14.12 Key Terms and Review Questions
   Key Terms
   Review Questions
14.13 References

Chapter 15: Threat and Incident Management
15.1 Technical Vulnerability Management
   Plan Vulnerability Management
   Discover Known Vulnerabilities
   Scan for Vulnerabilities
   Log and Report
   Remediate Vulnerabilities
15.2 Security Event Logging
   Security Event Logging Objective
   Potential Security Log Sources
   What to Log
   Protection of Log Data
   Log Management Policy
15.3 Security Event Management
   SEM Functions
   SEM Best Practices
15.4 Threat Intelligence
   Threat Taxonomy
   The Importance of Threat Intelligence
   Gathering Threat Intelligence
   Threat Analysis
15.5 Cyber Attack Protection
   Cyber Attack Kill Chain
   Protection and Response Measures
   Non-Malware Attacks
15.6 Security Incident Management Framework
Table of Contents

Objectives of Incident Management
Relationship to Information Security Management System
Incident Management Policy
Roles and Responsibilities
Incident Management Information
Incident Management Tools

15.7 Security Incident Management Process
   Preparing for Incident Response
   Detection and Analysis
   Containment, Eradication, and Recovery
   Post-Incident Activity

15.8 Emergency Fixes

15.9 Forensic Investigations
   Prepare
   Identify
   Collect
   Preserve
   Analyze
   Report

15.10 Threat and Incident Management Best Practices

15.11 Key Terms and Review Questions
   Key Terms
   Review Questions

15.12 References

Chapter 16: Local Environment Management

16.1 Local Environment Security
   Local Environment Profile
   Local Security Coordination

16.2 Physical Security
   Physical Security Threats
   Physical Security Officer
   Defense in Depth
# Table of Contents

Physical Security: Prevention and Mitigation Measures
Physical Security Controls

16.3 Local Environment Management Best Practices
16.4 Key Terms and Review Questions

Key Terms
Review Questions

16.5 References

Chapter 17: Business Continuity

17.1 Business Continuity Concepts
   Threats
   Business Continuity in Operation
   Business Continuity Objectives
   Essential Components for Maintaining Business Continuity

17.2 Business Continuity Program
   Governance
   Business Impact Analysis
   Risk Assessment
   Business Continuity Strategy

17.3 Business Continuity Readiness
   Awareness
   Training
   Resilience
   Control Selection
   Business Continuity Plan
   Exercising and Testing
   Performance Evaluation

17.4 Business Continuity Operations
   Emergency Response
   Crisis Management
   Business Recovery/Restoration

17.5 Business Continuity Best Practices
17.6 Key Terms and Review Questions
Table of Contents

Key Terms
Review Questions
17.7 References

Part III: Security Assessment

Chapter 18: Security Monitoring and Improvement

18.1 Security Audit
  Security Audit and Alarms Model
  Data to Collect for Auditing
  Internal and External Audit
  Security Audit Controls

18.2 Security Performance
  Security Performance Measurement
  Security Monitoring and Reporting
  Information Risk Reporting
  Information Security Compliance Monitoring

18.3 Security Monitoring and Improvement Best Practices

18.4 Key Terms and Review Questions
  Key Terms
  Review Questions

18.5 References

Appendix A: References and Standards
Appendix B: Glossary
Index
Appendix C: Answers to Review Questions