



FOURTH EDITION



DEVELOPING CYBERSECURITY PROGRAMS AND POLICIES IN AN AI-DRIVEN WORLD

OMAR SANTOS

Developing Cybersecurity Programs and Policies in an AI-Driven World

Fourth Edition

Omar Santos

PEARSON

Hoboken, New Jersey

Developing Cybersecurity Programs and Policies in an AI-Driven World

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Table of Contents

Introduction

Chapter 1: Understanding Cybersecurity Policy and Governance

Information Security vs. Cybersecurity Policies

Looking at Policy Through the Ages

Policy in Ancient Times

The U.S. Constitution as a Policy Revolution

Policy Today

Cybersecurity Policy

What Are Assets?

Characteristics of Successful Policy

What Is the Role of Government?

The Challenges of Global Policies

Cybersecurity Policy Life Cycle

Policy Development

Policy Publication

Policy Adoption

Table of Contents

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 Frameworks

Confidentiality, Integrity, and Availability (CIA)

What Is Confidentiality?

What Is Integrity?

What Is Availability?

Who Is Responsible for CIA?

What Is a Cybersecurity Framework?

What Is NIST's Function?

So, What About ISO?

Table of Contents

The Importance of ISO Standards for Cybersecurity

NIST Cybersecurity Framework

The Objective of the NIST Cybersecurity Framework

The Scope of the CSF

The NIST Framework Core Components

Implementation Examples and Informative References

The NIST Cybersecurity Framework and the NIST Privacy Framework

Summary

Chapter 4: Cloud Security

Why Cloud Computing?

Scalability vs. Elasticity

CostBenefit Analysis of Cloud Computing

Cloud Computing Models

Software as a Service (SaaS)

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Function as a Service (FaaS)

The Cloud Shared Responsibility Model

Cloud Governance

Centralized Control and Coordination

Standardization and Compliance

Preventing Shadow IT

The Role of Cloud Governance

Transferring Regulatory Responsibility and Costs to the Cloud

Multitenancy

Core Components of the Cloud Computing Reference Architecture

Key Concepts and Functional Layers of Cloud Computing

The Importance of the Reference Architecture

Table of Contents

Understanding Top Cybersecurity Risks in Cloud Computing

- Data Breaches and Loss

- Inadequate Identity and Access Management (IAM)

- Leveraging Identity Federation

- Automating the IAM Processes and Mitigating Associated Risks

- Misconfiguration and Inadequate Change Control

- Lack of Visibility and Control Over Data

- Insider Threats

- Advanced Persistent Threats (APTs) and Sophisticated Malware Against
Cloud-Based Solutions

AI and the Cloud: Revolutionizing the Future of Computing

Summary

Chapter 5: 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

- The European Union Cyber Resilience Act

Table of Contents

Cybersecurity Risk

Is Risk Bad?

Understanding Risk Management

Risk Appetite and Tolerance

What Is a Risk Assessment?

Risk Assessment Methodologies

Summary

Chapter 6: Asset Management and Data Loss Prevention

Information Assets and Systems

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 7: Human Resources Security and Education

The Employee Life Cycle

What Does Recruitment Have to Do with Security?

What Happens in the Onboarding Phase?

What Is User Provisioning?

Table of Contents

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

NICE Work Roles and Categories

NICE Insider Threat Analysis

Influencing Behavior with Security Awareness

Teaching a Skill with Security Training

Security Education Is Knowledge Driven

Summary

Chapter 8: Physical and Environmental Security

Understanding the Secure Facility Layered Defense Model

How Do We Secure the Site?

How Is Physical Access Controlled?

Protecting Equipment

The Importance of Power to Processing

How Dangerous Is Fire?

What About Disposal of Devices Containing Data?

Stop, Thief!

Environmental Sustainability

Summary

Chapter 9: Cybersecurity Operations (CyberOps), Incident Response, Digital Forensics, and Threat Hunting

Incident Response

What Is an Incident?

How Are Incidents Reported?

Table of Contents

What Is an Incident Response Program?

The Incident Response Process

Tabletop Exercises and Playbooks

Information Sharing and Coordination

Operationalizing Threat Intelligence

Computer Security Incident Response Teams (CSIRTs)

Product Security Incident Response Teams (PSIRTs)

Incident Response Training and Exercises

What Happened? Investigation and Evidence Handling

Documenting Incidents

Working with Law Enforcement

Understanding Threat Hunting

Objectives of Threat Hunting

The Threat Hunting Process

Best Practices for Threat Hunting

Using SIGMA for Incident Response and Threat Hunting

Understanding Digital Forensic Analysis

Data Breach Notification Requirements

Is There a Federal Breach Notification Law?

Does Notification Work?

Summary

Chapter 10: Access Control Management

Access Control Fundamentals

What Is a Security Posture?

How Is Identity Verified?

What Is Authorization?

Accounting

Infrastructure Access Controls

Table of Contents

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 11: Supply Chain Security, Information Systems Acquisition, Development, and Maintenance

Strengthening the Links: A Deep Dive into Supply Chain Security

Emerging Threats to Supply Chains

Strategies for Enhancing Supply Chain Security

The Critical Role of SBOMs in Enhancing Supply Chain Security

Artificial Intelligence Bill of Materials (AI BOM)

System Security Requirements

What Is SDLC?

NIST's Secure Software Development Framework (SSDF)

What About Commercially Available or Open Source Software?

The Testing Environment

Protecting Test Data

Secure Code

The Open Worldwide Application Security Project (OWASP)

Cryptography

Why Encrypt?

Regulatory Requirements

What Is a Key?

What Is PKI?

Why Protect Cryptographic Keys?

Digital Certificate Compromise

Table of Contents

Post-Quantum Cryptography: Securing the Future of Digital Security

Summary

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

Business Continuity and Disaster Recovery in Cloud Services

Key Components of BC/DR in Cloud Computing

Best Practices for BC/DR in Cloud Services

Business Continuity and Disaster Recovery Strategies in Cloud Computing
vs. Traditional Data Centers

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?

Table of Contents

Regulatory Oversight

What Are the Interagency Guidelines?

New Yorks Department of Financial Services Cybersecurity
Regulation

What Is a Regulatory Examination?

Examination Process

Examination Ratings

Personal and Corporate Identity Theft

What Is Required by the Interagency Guidelines Supplement A?

Authentication in an Internet Banking Environment

Regulation of Fintech, Digital Assets, and Cryptocurrencies

The Rise of Fintech and Digital Assets

Regulatory Responses

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 Administrative Safeguards?

What Are the Physical Safeguards?

What Are the Technical Safeguards?

What Are the Organizational Requirements?

What Are the Policies and Procedures Standards?

Mapping the HIPAA Security Rule to the 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

Table of Contents

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?

What Is a Data Security Compliance Assessment?

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

Are There Penalties for Noncompliance?

Summary

Chapter 16: Privacy in an AI-Driven Landscape

Defining Privacy in the Digital Context

The Interplay Between AI and Privacy

AI as a Privacy Protector and Challenger

Privacy Concerns in AI Applications

Privacy-Preserving Techniques in AI

General Data Protection Regulation (GDPR)

GDPR Key Principles

Impact on Businesses

Rights for Individuals

California Consumer Privacy Act (CCPA)

Key Provisions and Compliance Requirements of CCPA

CCPA vs. GDPR

Personal Information Protection and Electronic Documents Act

Table of Contents

(PIPEDA)

Data Protection Act 2018 in the United Kingdom

Comparing GDPR, CCPA, PIPEDA, and DPA 2018

Leveraging AI to Enhance Privacy Protections

Summary

Chapter 17: Artificial Intelligence Governance and Regulations

The AI Double-Edged Sword

Generative AI, LLMs, and Traditional Machine Learning

Implementations

Introduction to AI Governance

The U.S. Executive Order on the Safe, Secure, and Trustworthy
Development and Use of Artificial Intelligence

The Blueprint for an AI Bill of Rights

The Foundation of AI Governance: Guiding Principles from the Executive
Order

NISTs AI Risk Management Framework

Implementing the AI RMF

The Importance of High Accuracy and Precision in AI Systems

Explainable AI (XAI): Building Trust and Understanding

Tools for XAI

Government and Society-wide Approaches to AI Governance

The U.S. National AI Advisory Committee

The European Artificial Intelligence Board

A Society-wide Approach to AI Governance

The EU AI Act

Comparing U.S. Executive Order 14110 and the EU AI Act

Guidelines for Secure AI System Development

Key Guidelines from CISA and NCSC

Table of Contents

Provider and User Responsibility

AI Supply Chain Security

OWASP Top 10 Risks for LLM

Prompt Injection Attacks

Insecure Output Handling

Training Data Poisoning

Model Denial of Service

Supply Chain Vulnerabilities

Sensitive Information Disclosure

Insecure Plugin Design

Excessive Agency

Overreliance

Model Theft

Model Inversion and Extraction

Backdoor Attacks

MITRE ATLAS Framework

Summary

Appendix A: Answers to the Multiple Choice Questions

Index