Cyber Security

Index

Chapter 1: Best Practices in Cyber Security
1.1 Common Cyber Security Measures
1.2 Security Governance Principles
1.3 Components and Approaches of Cyber Security
1.4 Information Risk Management
1.5 Security Management Functions
1.6 Acceptable Use Policy
1.7 Security Management Best Practices
1.8 Security Models

Chapter 2: People Management
2.1 Human Resource Security
2.2 Information Classification
2.3 Records and Documents Management
2.4 Physical Asset Management
2.5 Office Equipment: Planning Considerations and Security Measures
2.6 Industrial Control System (ICS)
2.7 Mobile Device Security
2.8 Incorporation Security in SDLC
2.9 Disaster Management
2.10 Incident Response Plan

Chapter 3: Business Application Management
3.1 Introduction to Application Management
3.2 Corporate Application Security
3.3 End-User-Developed Applications
3.4 Access Control
3.5 Authentication Mechanisms
3.6 System Security Management
3.7 Virtual Servers
3.8 Network Storage System
3.9 Network Management

3.10 Firewall
3.11 IP Security (IPSec)
3.12 Electronic Communication

Chapter 4: Supply Chain Management
4.1 Introduction to Supply Chain Risk Management
4.2 Cloud Security
4.3 Security Architecture
4.4 Malware Protection: Types, Tools and Best Practices
4.5 Intrusion Detection System (IDS)
4.6 Digital Rights Management (DRM)
4.7 Cryptographic Techniques
4.8 Threat in Cybersecurity
4.9 Vulnerability Management Process
4.10 SIEM Capabilities and Applications
4.11 Cyber Forensics Investigations
4.12 Local Environmental Management
4.13 Business Continuity Management

Chapter 5: Security Monitoring and Improvement
5.1 The Importance of Cybersecurity Monitoring
5.2 Improvement Areas
5.3 Cybersecurity Audit
5.4 Security Performance
5.5 Information Risk Management
5.6 Compliance Management
5.7 Cyber Security Monitoring Services
5.8 Cybersecurity Best Practices for Security