Course Schedule - Topics & Activities

Cybersecurity Introduction & Overview

- Introduction to Cybersecurity
  - The evolution of Cybersecurity
  - Cybersecurity & situational awareness
  - The Cybersecurity skills gap
- Difference between Information Security & Cybersecurity
  - Protecting digital assets
- Cybersecurity objectives
  - Confidentiality, integrity, & availability
  - Nonrepudiation
- Cybersecurity roles
  - Governance, risk management, & compliance
  - What does a Cybersecurity professional do?
  - Information Security roles
  - Board of Directors
  - Executive management
  - Senior Information security management
  - Cybersecurity practitioners
- Cybersecurity domains
  - Cybersecurity concepts
  - Security architecture principles
  - Security of networks, systems, applications, & data
  - Incident response
  - Security implications & adoption of evolving technology

Cybersecurity Concepts

- Risk
  - Approaches to Cybersecurity
  - Key terms & definitions
  - Likelihood & impact
  - Approaches to risk
  - Third-party risk
  - Risk management
• Common attack types & vectors
  o Threat agents
  o Attack attributes
  o Generalized attack process
  o Nonadversarial threat events
  o Malware & attack types

• Policies & procedures
  o Policy life cycle
  o Guidelines
  o Policy frameworks
  o Types of Information Security policies
  o Access control policy
  o Personnel Information Security policy
  o Security incident response policy

• Cybersecurity controls
  o Identity management
  o Provisioning & de-provisioning
  o Authorization
  o Access control lists
  o Privileged user management
  o Change management
  o Configuration management
  o Patch management

Security Architecture Principles

• Overview of security architecture
  o The security perimeter
  o Interdependencies
  o Security architectures & frameworks
  o SABSA & the Zachman framework
  o The open group architecture framework (TOGAF)

• The OSI model
  o TCP/IP

• Defense in Depth

• Firewalls
  o Firewall general features
  o Network firewall types
  o Packet filtering firewalls
• Stateful inspection firewalls
  • Stateless vs. stateful
  • Examples of firewall implementations
  • Firewall issues
  • Firewall platforms

• Isolation & segmentation
  • VLANs
  • Security zones & DMZs

• Monitoring, detection, and logging
  • Ingress, egress, & data loss prevention (DLP)
  • Antivirus & anti-malware
  • Intrusion detection systems
  • IDS limitations
  • IDS policy
  • Intrusion prevention systems

• Cryptography Fundamentals
  • Key elements of cryptographic systems
  • Key systems

• Encryption techniques
  • Symmetric (private) key encryption
  • Asymmetric (private) key encryption
  • Elliptical curve cryptography
  • Quantum cryptography
  • Advanced encryption standard
  • Digital signature
  • Virtual private network
  • Wireless network protections
  • Stored data
  • Public key infrastructure

• Encryption applications
  • Applications of cryptographic systems

**Security of Networks, Systems, Applications, & Data**

• Process controls – risk assessments
  • Attributes of risk
  • Risk response workflow
  • Risk analysis
  • Evaluating security controls
risk assessment success criteria
Managing risk
Using the results of the risk assessment

- Process controls – vulnerability management
  - Vulnerability management
  - Vulnerability scans
  - Vulnerability assessment
  - Remediation
  - Reporting & metrics

- Process controls – penetration testing
  - Penetration testers
  - Penetration testing phases

- Network security
  - Network management
  - LAN/WAN security
  - Network risks
  - Wireless local area networks
  - Wired equivalent privacy & Wi-Fi protected access (WPA/WPA2)
  - Ports & protocols
  - Port numbers
  - Protocol numbers & assignment services
  - Virtual private networks
  - Remote access

- Operating system security
  - System/platform hardening
  - Modes of operations
  - File system permissions
  - Credentials & privileges
  - Command line knowledge
  - Logging & system monitoring
  - Virtualization
  - Specialized systems

- Application security
  - System development life cycle (SDLC)
  - Security within SDLC
  - Design requirements
  - Testing
  - Review process
- Separation of development, testing, & production environments
- OWASP top ten
- Wireless application protocol (WAP)

- Data security
  - Data classification
  - Data owners
  - Data classification requirements
  - Database security

**Incident Response**

- Event vs. incident
  - Events vs. incident
  - Types of incidents

- Security incident response
  - What is incident response?
  - Why do we need incident response?
  - Elements of an incident response plan
  - Security event management

- Investigations, legal holds, & preservation
  - Investigations
  - Evidence preservation
  - Legal requirements

- Forensics
  - Data protection
  - Data acquisition
  - Imaging
  - Extraction
  - Interrogation
  - Ingestion/normalization
  - Reporting
  - Network traffic analysis
  - Log file analysis
  - Time lines
  - Anti-forensics

- Disaster recovery & business continuity plans
  - What is a disaster?
  - Business continuity & disaster recovery
  - Business impact analysis
Recovery time objectives (RTO)
Recover point objective (RPO)
IS business continuity planning
Recovery concepts
Backup procedures

Security Implications & Adoption of Evolving Technology

- Current threat landscape
- Advanced persistent threats (APTs)
  - Evolution of the threat landscape
  - Defining APTs
  - APT characteristics
  - APT targets
  - Stages of an APT attack
- Mobile technology – vulnerabilities, threats, & risk
  - Physical risk
  - Organizational risk
  - Technical risk
  - Activity monitoring & data retrieval
  - Unauthorized network connectivity
  - Web view/user interface (UI) impersonation
  - Sensitive data leakage
  - Unsafe sensitive data storage
  - Unsafe sensitive data transmission
  - Drive-by vulnerabilities
- Consumerization of IT & mobile devices
  - Consumerization of IT
  - BYOD
- Cloud & digital collaboration
  - Risk of cloud computing
  - Web application risk
  - Benefits of cloud computing