Cyber Security for Small and Medium Businesses

Duration: 5 Days *(Face-to-Face & Remote-Live)*, or 35 Hours *(On-Demand)*

Price: CDN$3,275 *(Face-to-Face & Remote-Live)*, or CDN$1,995 *(On-Demand)*

Discounts: We offer multiple discount options. Click here for more info.

Delivery Options: Attend face-to-face in the classroom, remote-live or on-demand training.

Students Will Learn

- How to create a secure IT environment
- To assess risk
- How to manage the risks associated with firewall, servers and routers
- The use of certificate and digital signatures
- How to build policies, procedures, standards, guidelines and controls
- To implement user account security
- How to respond to incidents
- To understand and assess social media threats, methods, and techniques
- Recovery planning and methods
- To undertand and manage issues related to patch management and other software vulnerabilities
- How to build monitoring capability to identify security trends or issues
- The laws, rules and regulations with which enterprises must and/or should comply

Course Description

The Cyber Security for Small and Medium Businesses course provides a practical overview of the cyber security issues faced today by enterprises of all shapes and sizes, and teaches students how to protect their enterprise data. The course covers how to identify risks, monitor computers and networks for breaches, implement security policies, deploy tools to secure systems, and plan for all scenarios.

Upon completion of the course, students will be able to identify vulnerabilities and design and implement security polices and systems. They will also have a solid foundation regarding laws, rules and regulations that pertain to cyber security, as well as an understanding of available tools (mostly public domain or low cost) for monitoring and securing systems.

Course Prerequisites

Fundamental knowledge of computer operations and networking.

Course Overview

The Human Factors of Security

- What Is Risk?
  - What You Can Do to Reduce Risk
  - Four Processes
  - The CIA of Security
- The Company Manual: What's in It
- Defining Security Policy
  - Policies, Procedures, Standards, Guidelines and Controls
- Developing Electronic Policy

Objectives of Security

- Security: Why and How
- Basic Networking Technology
- Overview of TCP/IP
- Ports
- Mapping a Network
- Baselines

Active Directory

- Central Management vs. Standalone Management
- Standalone
  - Why?
  - Drawbacks
- Fundamentals of Active Directory
  - Roles
  - Drawbacks
  - Group Policies
  - Backing up Active Directory

What Hackers Know

- The Social and Web Views of Your Enterprise
- Public and Private Information
- How to Analyze Your Web Presence
- Hidden Issues
- ID Issues
- Web Logs
- Web Crawlers

Perpetrators and Their Motivators

- You, Your Employees and Social Engineering
- Defense against Phishing
  - Examples of Phishing
- Certificates
  - Certificate Authorities
  - Building a CA
- Digital Certificates and Email
- Deploying Digital Certificates

Assessing Vulnerabilities (Before the Enemy Does)

- Patch Management on Devices and Computers
- Authentication for Credentials
  - PAP
  - CHAP
  - EAP
- Weak Passwords
  - Defaults Passwords
  - Standard Password Configurations
- Two-Factor Solutions
  - Biometrics
  - Card and Pin

Regulatory Issues and Action Items

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- General Data Protection Regulation (GDPR)

Viruses, Malware and Ransomware

- Viruses
- Worms
- Trojans
- Malware
- Ransomware
- Defense Against the Dark Arts

- Health Insurance Portability and Accountability Act (HIPAA)
- NY DFS Cybersecurity Regulation (23 NYCRR 500)

Disaster Recovery (DR) and Business Continuity Planning (BCP)

- A True Disaster
- Disaster Recovery
- Business Continuity Planning
- Requirements for DR and BCP
- Contents of Disaster Recovery and Business Continuity Plans
- Building a Disaster Recovery Plan
- Building a Business Continuity Plan

Support Groups and Sites

- InfraGuard
- SBA
- FTC
- ISACA
- Local Groups
- Your Support Company

Frameworks and GRC

- Frameworks
  - NIST
  - CSF
  - RMF
- Tools
  - The DHS CSET Tool
- GRC
- A Risk Register

Onboarding Employees

- Before Hire
  - Background Check
  - Reference Check
- At Hire
  - Reviewing the Company Manual
  - Policies with Regard to Web Use, Email and SPAM
- Training End Users

Backups

- Types and Trade-Offs
  - Full
  - Incremental
  - Differential
- Disk-Based
- Cloud-Based

Auditing for Compliance and Verification

- Controls
  - Technical
  - Physical
  - Administrative
- Employing Audits
  - Internal Audits
  - External Audits

Monitoring

- Benefits
- Targets
  - Servers
  - Bastion Hosts
  - Routers, Firewalls and Switches
  - Web Sites
  - Workstations
  - Networks (IDS, IPS)
- Tools
  - Tripwire
  - CIMTRAK
  - Security Information and Event Management (SIEM)
- Building a Monitoring System

Incident Investigation

- Defining Incidents and Events
- Before the Investigation
- Incident Investigation Methods
- Forensics
- Chain of Custody

Contacts

Networking

- Ethernet
  - Architecture
  - MAC Addresses
  - Network Traffic
  - Wireshark
  - FTP
- Protecting Network Traffic
  - IPSEC
- WIFI
  - WIFI Encryption: WEP, WPA, WPA2, WPA3
  - Hacking a WIFI Network
- Virtual Private Networks
  - Tunnels
  - SSL
  - Microsoft Direct Access
  - Securing VPNs

Physical Security

- Server Protection
- Workstation Protection
- Locking Down Stations
- The Physical Plant
  - Office Access
  - Server Access
  - Network Policies
  - Material Security
- Outside the Office
  - Laptops
  - Remote Devices
  - Encrypting Hard Drives
  - Smart Phones
  - Anti-Virus Software

Change Management

- Definitions
- Adaptation and Methods

Hands On Technology Transfer
The Best Way to Transfer Technology Skills

1 Village Square, Suite 8
14 Fletcher Street
Chelmsford, MA 01824