Cybersecurity for Managers

Conatum Consulting LLC
Bernard S. Donefer

"Early retirement" The highlight of a successful career or a euphemism for making a quick exit after a cybersecurity breach? Recent events demonstrate that governments and businesses of all sizes are vulnerable to attack from diverse adversaries. Intellectual property stolen, privacy violated, operations disrupted -- incidents that drive up costs, reduce sales, impact innovation and inflict reputational damage.

Have you taken sufficient measures to prevent an attack or recover from one in a timely manner? What more can be done?

No class, product or security framework can ensure you will never suffer the effects of a cyber hack. You can, however, achieve and improve oversight.

This class is intended for all levels of management responsible for ensuring that all reasonable steps are taken to withstand, blunt and recover from any cyber incident. You will become familiar with national recommended standards such as the NIST Cybersecurity Framework and the Lockheed Cyber Kill Chain and how they may apply to your situation. You will return to your office with a list of questions whose answers will either prioritize further efforts or raise your confidence in your firm's preparedness.

Agenda

1. Recent cases, e.g. Target and Equifax
    a. What happened, red flags, governance issues, lessons learned?
    b. What could have done to have prevented these incidents?
2. Governance
    a. Security in support of the mission
        i. Economics and costs of security
    b. Roles and responsibilities
        i. Tiered risk management
        ii. Internal and external audit
        iii. Organizational issues and culture
3. Regulation and guideline - industry specific
    a. EU GDPR privacy
        i. Privacy vs. security
        ii. Data collection and its usage
    b. SCI securities industry
    c. HIPPA hospitals and medical services
    d. FFEIC banking
    e. PCI DSS credit cards

4. Types of attacks
    a. Social engineering
        i. Pfishing, spear pfishing and whaling
    b. Malware
        ii. Key loggers, trojans, viruses, ransomware
        iii. Back doors, zombie machines, botnets
    c. Zero day exploits
    d. Denial of service (DDOS)
5. Perimeter protection
    a. Air gapping and the Stuxnet virus attack
    b. Firewalls, VPNs, anti-virus
    c. Intrusion detection and prevention systems (IDS, IPS)
        iv. Unified Threat Management (UTM)
    d. DNC and JPMorgan Chase attacks
6. Sources of attack and defense
    a. Types of attackers and their objectives
    b. The Cyber Kill Chain for Advanced Persistent Threats (APT)

1. Reconnaissance	5. Installation
2. Weaponization	6. Command and Control
3. Delivery	7. Actions on Objective
4. Exploitation	

7. Authentication and access control
    a. Estonia – example of national e-id
    b. Digital identification
    c. Authentication and assurance
    d. Two factor and multifactor authentication
    e. Best practices in passwords
    f. Role and attribute based access control policies
8. The Cloud
    a. Cloud deployment – private, community, public
    b. Service models
        v. Software, platform or infrastructure as service
    c. Vendor security and service level responsibilities
    d. Client security responsibilities
9. Operational risk
    a. Control Self-Assessment
    b. Key Risk Indictors
    c. Risk dashboard – control points
10. Risk Security Frameworks
    a. Department of Homeland Security
    b. National Institute of Standards and Technology (NIST) Framework
    c. ISO
    d. COBIT 5
    e. US Computer Emergency Readiness Team CERT

11. Return to work to-do list
    a. Four Questions of Cybersecurity
        1. What and who are you trying to protect? Your priorities
        2. How do protect those assets? What are you protecting against? What defenses to put in place? How to mitigate social engineering?
        3. How do you know if you are being attacked or if your defenses have been successfully penetrated?
        4. How to respond to the attack and mitigate any damage? Communication