Bootcamp PPT#4

Session 2.1 Governance, Risk, and Compliance I

Thursday September 10, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

GRC: Security Within an Organization

- Identify 3 concrete benefits of a healthy security culture.
- Responsibitilty of C Suite Officers and CISO Roles.
- Security department roles responsibilities.
- Identify appropriate security controls for a given resource and situation.

Security Aligning within an Organization

- Tools for techincal roles.
- Soft Skills in demand.
- **Linux and Windows**
  - Managing users, permissions, scheduling tasks, manage installed software with **apt**.
- **Networking**
  - Configure firewalls, port scan remote hosts, analyze network traffic.
- **Web Vulnerabilities and Web Services**
  - Burp Suite
- **Offensive Security**
- **Defensive Security**
- Security Concerns VS Business Concerns
  - **Security Goal:** Protect data. (Improve **security posture**.)
    - **Passive** VS **Defensive**
  - **Business Goal:** Maximize profit and improve efficiency.
  - Balance of **adequate protection** for important **assets**.
- **GRC Framework**
  - **Governance:** Creating management **processes for implementing security practices**.
  - **Compliance:** Making sure the business follows **internal security policies**.
  - **Risk Management:** Identifying an organizations most important **assets** and determining

how the might be **compromised**.

Security Culture and Framework

- Security Culture is the way members of an organization think about and approach security issues.
- How important or aware with regard to security are employees?
- **How to Motive Employees within a Culture Framework:**
  - Measure and Set Goals
    - Phishing email campaign with statistical expectations.
  - Involve the Right People
    - Inform Management
  - Create an Action Plan
    - Develop Training
  - Execute the Plan
    - Deploy training
  - Measure the Change
    - Phishing email campaign with statistical expectations.
- Encourage people, don't punish them.

Example Roles

- **CEO:** Chief Executive Officer
- **CFO:** Chief Financial Officer
- **COO:** Chief Operations Officer
- **CISO:** Chief Information Security Officer
- **CIO:** Chief Information Officer
- **CTO:** Chief Technology Officer

Reporting Structure

- **Network Engineer** reports to...
- **Performance Manager** reports to...
- **Director of IT** reports to...
- **VP of Networking**

Responsibilities

- Director of Networking
- IR or SOC Manager
- Security Architect

Security Controls

- Long term vs Short term
- **Security Control:** system processes or technology that protects CIA model.
    - **Preventative**
    - **Deterrent**
    - **Detective**
    - **Corrective**
    - **Compensating**
- **Access Points for Servers**
    - **VPN**
    - SSH protocol and **keys** and **passwords**.
    - Strong **updated passwords**.
- **Control Diversity**
    - Firewall VPN.
    - Authentication of keys and passwords.
    - Limited time of compromise.
- **Redundancy** and Single Points of Failure
    - Multiple methods in case one fails