Intro to Security

How does security relate to information security?

Security: *to be free from danger, and the process to achieving that goal.*

- As security increases, convenience often decreases

Information security: *securing information in a digital format.*

- *maniupulated data* - data-in-use
- *preserved data* - data-at-rest
- _transmitted data** - data-in-transit

Goal To ward off attacks, & prevent total collapse when an attack is successful.

Purpose:

- *prevent* data theft
- *thwart* identity theft
- avoid *legal consequences* of not securing information
- maintain *productivity*
- *foiling* cyber-terrorism

Roles

- *Security Administrator*: Analyze and design security solutions as well as identifying users' needs
  - does **NOT** report directly to the CIO
- *Security Manager*: Reports directly to the CISO, and supervises technicians, admins, and security staff
- *Security Analyst*:
  - Job growth to be 18% by 2024
- *Security Technician*: Entry-level position
- CSO
- CIO
- CSIO

Three types of **information protection**:

- *Confidentiality* - access via approval
- *Integrity* - correct & unaltered
- _Availability** - authorized access

Security Layers:

- Information
  - Processed
  - Stored

    - Transmitted
- Traits
    - Confidentiality
    - Integrity
    - Availability
- Layers
    - Products
    - People
    - Policies & Procedures
- *Products* form the actual security mechanism for the data
- *People* implement and use the products to protect the data
- *Policies & Procedures* maintain the proper use of products

> An immediate solution that cuts through the complexity of a problem is called a _“silver bullet”**

Technical Controls: The process of using technology as a basis for controlling usage and access to sensitive data.

5 Fundamental Security Principals

- *Layering* - most comprehensive, “defense-in-depth”

- *Limiting* - file permissions, or controlling human behavior via policy

- *Diversity* - layers must be from different vendors - “vendor diversity”

- *Obscurity* - not revealing any details about products used

- *Simplicity* - hardened designs, like a 50 cal

- industry standard frameworks and reference architectures give broad guidance about a security framework

    - regulatory frameworks are required by external agencies
    - industry-specific frameworks address a particular sector; i.e. finance vs. power grid
    - some are globally designed, others specific to a region
    - Common frameworks include ISO, COBIT, RFC (FIXME)

> Information security **protects and establishes** CIA on devices that *store, process, and transmit* data; by using *products, people, and procedures.*

- *Asset*: item that has value
- *Threat*: type of action that has potential to cause harm
- *Threat Actor*: person (or element) with power to carry out a threat
- *Vulnerability*: flaw or weakness that allows threat actor to bypass security
- *Attack / Threat Vector*: means by which an attack can occur

- *Risk*: situation that involves exposure to danger
- *Likelihood*: probability that vulnerability is exploited

Risk Response Techniques

- *Accept* - do nothing to address the risk
- *Transfer* - make 3rd party deal with it
- *Avoid* - don't involve yourself in the actions that exposed yourself to the risk
- _Mitigate** - address and reduce the risk

Types of Theft:

- *Enterprise Data Theft*: proprietary business information
- *Personal Data Theft*: credit card number, SSN
- *Identity Theft*: use SSN and identity to open a credit card

Laws Protecting Privacy

- *HIPAA* ~ health insurance portability & accountability act (1996)
  - confidentiality of health reports
-
  ### *Sarbanes-Oxley* act of 2002 (Sarbox)
- *Gramm-Leach-Bliley* act (GLBA)
  - Requires banks and financial institutions to alert their customers of policies and practices in reporting and disclosing customer info
- Payment Card Industry Data Security Standard (PCI DSS)
  - Policies that force merchants to properly store their customer's credit card info, and to routinely test their systems
- State notification & Security Laws
  - California's Database Security Breach Notification act (2003)

Reasons for Widespread Vulnerabilities

- Large number of vulnerabilities
- End-of-life systems
- Lack of vendor support

Reasons it's difficult to defend

- Delays in security updating
- Increased speed of attacks
- Simplicity of attack tools

> Vulnerable business processes, also called business process compromise (BPC), occurs when an attacker manipulates commonplace actions that are routinely performed within an organization.

Cyber-Crime

Two types of cyber crime: one focuses on individuals, the other on enterprises & governments.

> Varies by funding & resources available to threat actors, whether originated by internal or external entities, and by their intent.

Cyber-Terrorism: Any premeditated, politically motivated attack against information, computer systems, computer programs, and data.

- cause panic, provoke violence, ruin finances
- banking industry, military, power plants, air traffic control, water systems

> The most dangerous attackers attack the sustainability of life

Script Kiddies: Just motivated noobs. > 40% of attacks are by noobs.

- 13% no skill
- 28% little skill
- 44% moderate skill
- 15% high skill

Hacktivist: Soy-boy trying to make a statement

Nation-State Actor: James Bond of hacking, sponsored by a government

Advanced Persistent Threat: Multi-year campaign - a russian spy

> > 58% are inside jobs

Open-Source Intelligence: Automated attack software

Threat Actors

- *competitors* - Pepsi vs. Coke
- *organized crime* - online gambling scams
- *brokers* - sells knowledge of vulnerabilities
- *cyber terrorists* - attack power grids, etc.