Information Security for Managers

Workman, Phelps, Gathegi

Security Management

Goal of Security Management

Keep company profitable

To do this, Security Management Includes

- Security and well-being of employees
- Computer security
- Network security
- Information security

Computer Security

Securing computing devices such as

- Laptops
- Desktop computers
- Tablets
- Cell phones

Also includes personnel policies related to the use of these devices

Network Security

Securing the communication infrastructure, including

- Servers
- Routers
- Switches
- Firewalls
- Physical media (cabling and Wi-Fi devices)

Also includes personnel policies about using the network

Threats & Attacks

Definitions for now

Threat The POTENTIAL for a security breach due to vulnerabilities

Attack The actual EXPLOITATION of a vulnerability

Attacks can be PASSIVE or ACTIVE

Passive Attack Victim doesn't realize attack occurred
Example: Stolen information

Active Attack Disrupt operation in some way
Examples: Corrupt data, DOS

Incidents

Incidents encompass:

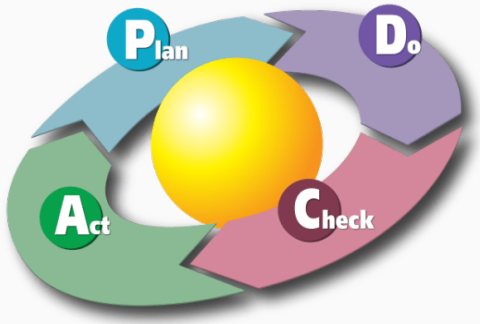
Attacks

Accidents Click on email link. didn't call JULIE before you dug

Natural Disasters Hurricane, flooding, etc.

Information Security Management Life Cycle (ISMLC)

1. Plan
2. Do
3. Check
4. Act



---

https://frsecure.com/blog/information-security-life-cycle-not-information-security-projects/

ISMLC — Plan: Think Things Through

Involve

- Senior management
- Stake holders
- Department managers

Actions

- Get management buy-in
- Form oversight/steering committee
- Determine business needs
- Determine threat profile
- Understand organization's risk tolerance

ISMLC — Do: Execute the Plan

Actions

- Assign specific responsibilities to individuals (roles & responsibilities)
- Determine deliverables and
- Develop Policies, Standards, Procedures, Guidelines
- Implement solutions
- Establish measurable metrics (are things getting better or worse)

ISMLC — Check: Is the Plan Working

Actions

- Make sue procedures are being followed (otherwise how can you know if the plan is working)
- Conduct audits

ISMLC — Act: Based on Audits

Actions

- Review audit results and collected metrics
- Meet quarterly with steering committee
- Recommend changes to the plan or its implementation

Working Away From the Office

Things not covered in this class

Covered in CSCI-640, Legal and Ethical Issues in IT Management

- Legal implications of expanding the "workplace"
- Liability issues related to extending the "Work Space" to "Personal space"

For us...

- Policies about securing assets while away from the office
  - Use of public Wi-Fi, home networks, VPN
  - Save locally vs. save to the cloud
  - Personal devices vs. company-owned devices
  - Use of corporate assets for personal activities
  - Encryption requirements