Information Security for Managers

Workman, Phelps, Gathegi

What's a Manager to Do

Managers are caught between

- Containing costs

What's a Manager to Do

Managers are caught between

- Containing costs
- Containing risk exposure

What's a Manager to Do

Managers are caught between

- Containing costs
- Containing risk exposure

Responsible for keeping business profitable

What's a Manager to Do

Managers are caught between

- Containing costs
- Containing risk exposure

Responsible for keeping business profitable

Protect workforce & corporate assets

What's a Manager to Do

Managers are caught between

- Containing costs
- Containing risk exposure

Responsible for keeping business profitable

Protect workforce & corporate assets

Formulate policies, procedures, practices

Internal vs. External

Attacks can come from within an organization (internal)

OR

Outside of the organization (external)

Definitions

Risk The potential for harm or damage to be caused to people or assets from a potential threat.

Definitions

Risk The potential for harm or damage to be caused to people or assets from a potential threat.

Governance Use of best practices, standards, and requirements to reduce risks.

Regulated Content

HIPAA **Health Insurance Portability and Accountability Act**

Health care providers required to secure PHI (protected health information)

Regulated Content

HIPAA **Health Insurance Portability and Accountability Act**

Health care providers required to secure PHI (protected health information)

FERPA **Family Educational Rights and Privacy Act**

Gives parents access to their child's education records
At age 18, rights transfer to the student

Regulators & Requirements

FRA Federal Records Act

Prevents shredding/deleting some emails

Regulators & Requirements

FRA **Federal Records Act**

Prevents shredding/deleting some emails

NARA **National Archives and Records Administration**

Falls under FRA

Regulators & Requirements

FRA **Federal Records Act**

Prevents shredding/deleting some emails

NARA **National Archives and Records Administration**

Falls under FRA

Managers may be required to

- Perform risk analysis

Regulators & Requirements

FRA **Federal Records Act**

Prevents shredding/deleting some emails

NARA **National Archives and Records Administration**

Falls under FRA

Managers may be required to

- Perform risk analysis
- Conduct threat and vulnerability assessments

Regulators & Requirements

FRA **Federal Records Act**

Prevents shredding/deleting some emails

NARA **National Archives and Records Administration**

Falls under FRA

Managers may be required to

- Perform risk analysis
- Conduct threat and vulnerability assessments
- Create plans for risk mitigation, disaster recovery, business continuity, etc.

Regulators & Requirements

FRA **Federal Records Act**

Prevents shredding/deleting some emails

NARA **National Archives and Records Administration**

Falls under FRA

Managers may be required to

- Perform risk analysis
- Conduct threat and vulnerability assessments
- Create plans for risk mitigation, disaster recovery, business continuity, etc.
- Conduct criminal forensic analysis

Cost - Direct Losses

- Loss – Stolen IP
- Loss – Lost business

Cost - Lawsuits

- Downstream lawsuits
- Upstream lawsuits

Free Speech vs. Due Process

- Free Speech - Free to post anything online
- Due Process - Respond to damage resulting from that speech

Free Speech vs. Due Process

- Free Speech - Free to post anything online
- Due Process - Respond to damage resulting from that speech

Due Process can take long $\longrightarrow$ SLAPP

Strategic Lawsuits Against Public Participation

Asset Planning - What Needs to be Protected

1. Enumerate assets (and their value)
2. Prioritize the assets (CIA)
    2.1 Confidentiality
    2.2 Integrity
    2.3 Availability
3. Determine how to protect assets

Asset Planning - What Needs to be Protected

1. Enumerate assets (and their value)
2. Prioritize the assets (CIA)
    2.1 Confidentiality
    2.2 Integrity
    2.3 Availability
3. Determine how to protect assets

Very tedious and time-consuming

Asset Planning - What Needs to be Protected

1. Enumerate assets (and their value)
2. Prioritize the assets (CIA)
    2.1 Confidentiality
    2.2 Integrity
    2.3 Availability
3. Determine how to protect assets

Very tedious and time-consuming

Methodologies such as FIPS (Federal Information Processing Standards) can help

Recognizing an Attack

IDS – Intrusion Detection Systems (Wireshark & SNORT)