Protection of Information Assets
- Week 2 -

Understanding an Organization’s Risk Environment
MIS5206 Week 2

• In the News
• Readings
• Understanding an Organization’s Risk Environment
• Test Taking Tip
• Quiz
• Next week
In the News

https://www.theregister.co.uk/2017/09/05/taringa_data_breach/


http://www.informationsecuritybuzz.com/expert-comments/vulnerabilities-found-nearly-half-million-pacemakers/


https://www.equifaxsecurity2017.com

In the News

https://www.govinfosecurity.com/instagram-warns-hack-more-widespread-than-expected-a-10256

http://www.theregister.co.uk/2017/09/01/police_cant_keep_license_plate_data_scans_secret/


https://www.theregister.co.uk/2017/09/05/lenovo_gets_wristslap_from_ftc_for_superfish_adware_debacle/


https://www.govinfosecurity.com/lenovo-ftc-to-settle-superfish-adware-complaint-a-10259


https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/


https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?mcubz=1


https://www.consumer.ftc.gov/blog/2017/08/taxslayer-file-one-under-authentication
In the News

http://www.theregister.co.uk/2017/08/31/pci_compliance_survey_verizon/
http://www.informationsecuritybuzz.com/expert-comments/vulnerabilities-found-nearly-half-million-pacemakers/
Reading

- Vacca Chapter 1
- ISACA RiskIT Framework pp. 1 - 42
- NIST Reading 1: “Framework for Improving Critical Infrastructure Cybersecurity”
The value of business’ data is at a peak

“A generation ago the asset base of US public companies was more than 80% tangible property” (e.g. raw materials, real estate, railroad cars...)

“Today... intangibles... account for more than 80% of listed company value”

Vacca 3rd Edition, pp. 3-4
Information Security Transformation

1970 data security examples
  – Guarding the photocopier
  – Watching who went in and out of the front door

Today’s data security must consider
  – Devices able to grab gigabytes of data and move them anywhere in the world in an instant
  – Laptops, tablets and smartphones with direct connection to company data are endpoints in a global network, creating thousands to millions of “front doors” leaving industry at its most vulnerable
One thing has not changed over the years...

*Human beings remain the primary vector for loss of corporate value*

*AND*

*Humans also control the processes and technologies central to information security function that preservers corporate value*
Information security means protecting information and information systems from:

- Unauthorized access, use, disclosure  \textbf{Confidentiality}
- Modification  \textbf{Integrity}
- Disruption and destruction  \textbf{Availability}
Key concepts

**Threat**
Potential for the occurrence of a harmful event such as an attack

**Vulnerability**
Weakness that makes targets susceptible to an attack

**Risk**
Potential of loss from an attack

**Risk Mitigation**
Strategy for dealing with risk
What is a threat?

Any thing that has the potential to lead to:

- *Unauthorized access, use, disclosure*
- *Modification*
- *Disruption or Destruction*

of an enterprises’ information
What is a threat...

Threats to information and information systems include:

- Purposeful attacks ("Human malicious")

- Human errors ("Human ignoramus")

- Structural Failures

- Environmental disruptions
## Taxonomy of threat sources

<table>
<thead>
<tr>
<th>Type of Threat Source</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADVERSARIAL</td>
<td>Individuals, groups, organizations, or states that seek to exploit the organization’s dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).</td>
<td>Capability, Intent, Targeting</td>
</tr>
<tr>
<td>ACCIDENTAL</td>
<td>Erroneous actions taken by individuals in the course of executing their everyday responsibilities.</td>
<td>Range of effects</td>
</tr>
<tr>
<td>STRUCTURAL</td>
<td>Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.</td>
<td>Range of effects</td>
</tr>
<tr>
<td>ENVIRONMENTAL</td>
<td>Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).</td>
<td>Range of effects</td>
</tr>
</tbody>
</table>
# Taxonomy of cybersecurity threat sources

<table>
<thead>
<tr>
<th>Type of Threat Source</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADVERSARIAL</td>
<td>Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).</td>
<td>Capability, Intent, Targeting</td>
</tr>
</tbody>
</table>

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66

**MIS 5206 Protecting Information Assets**
Anatomy of an Attack

I. Social engineering techniques target specific individuals
   Spear-phishing is a common technique used to lure targeted users into downloading initial-stage malware.

II. Establish a beachhead
   Initial-stage malware executes shellcode and calls home for further instructions.

III. Infiltration
   Custom executables with objective-specific malware is downloaded.
   Remote commands are executed according to attacker objectives.

IV. Persistence
   Attackers wait for opportune attack times. "Sleep" commands are often executed between "run" commands to avoid detection.

V. Accomplish Objectives (data harvesting, sabotage, and more)
   Remote commands issued to extract data, modify applications, or sabotage systems.

(McAfee, 2011)
Anatomy of an Attack

1. Attacker sends spear fishing e-mail
2. Victim opens attachment
   - Custom malware is installed
3. Custom malware communicates to control web site
   - Pulls down additional malware
4. Attacker establishes multiple backdoors
5. Attacker accesses system
   - Dumps account names and passwords from domain controller
6. Attacker cracks passwords
   - Has legitimate user accounts to continue attack undetected
7. Attacker reconnaissance
   - Identifies and gathers data
8. Data collected on staging server
9. Data exfiltrated
10. Attacker covers tracks
    - Deletes files
    - Can return any time

Advanced threats usually maintain remote access to target environments for 6-18 months before being detected (i.e. they are persistent) (Holcomb & Stapf, 2014)
Threat landscape

Anatomy of Advanced Persistent Threats (APT)\textsuperscript{19,20,21} to CII systems

Advanced threats usually maintain remote access to target environments for 6-18 months before being detected\textsuperscript{22}
### Taxonomy of cybersecurity threat sources

<table>
<thead>
<tr>
<th>Type of Threat Source</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCIDENTAL</td>
<td>Erroneous actions taken by individuals in the course of executing their everyday responsibilities.</td>
<td>Range of effects</td>
</tr>
<tr>
<td>- User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Privileged User/Administrator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66
Human non-malicious threat examples

- Computer operator errors
- Data entry (input) errors
- Inadequate access controls
- Inadequate training
- Inadequate human resource policies
- Inadequate program testing/controls incorporated into computer programs
- Inadequate risk analysis undertaken
- Inadequate supervision
- Lack of ethics
- Mislaid disk files
- Physical damage to disk
- Poor management philosophy/attitude
- Unlocked trash containers
- Update of wrong file
- Weak internal controls
## Taxonomy of cybersecurity threat sources

<table>
<thead>
<tr>
<th>Type of Threat Source</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRUCTURAL</td>
<td>Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.</td>
<td>Range of effects</td>
</tr>
<tr>
<td>- Information Technology (IT) Equipment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Display</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Controller</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Environmental Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Temperature/Humidity Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Power Supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Operating System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- General-Purpose Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Mission-Specific Application</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66
Structural Threat Examples

- Air conditioning failure
- Building collapse
- Destruction of data, disks, documents, reports
- Destruction of water mains, sewer lines
- Failure of hardware
- Failure of fire alarms, smoke detectors
- Failure of computer programs
- Freak accidents
- Gas line explosions
- Power outages (brownouts, blackouts, transients, spikes, sags and power surges)
- Product failure
- Software failure (operating system, database software)
Taxonomy of cybersecurity threat sources

<table>
<thead>
<tr>
<th>Type of Threat Source</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENVIRONMENTAL</td>
<td>Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).</td>
<td>Range of effects</td>
</tr>
<tr>
<td>- Natural or man-made disaster</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fire</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Flood/Tsunami</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Windstorm/Tornado</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Hurricane</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Earthquake</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Bombing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Overrun</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unusual Natural Event (e.g., sunspots)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Infrastructure Failure/Outage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Telecommunications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Electrical Power</td>
<td></td>
</tr>
</tbody>
</table>

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66
What is a Vulnerability?
What is a Vulnerability?

Any unaddressed susceptibility to a Physical, Technical or Administrative information security threat

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
What is a Risk?

A measure of threat

Potential loss resulting from unauthorized:
- Access, use, disclosure
- Modification
- Disruption or destruction

...of an enterprises’ information

Can be expresses in quantitative and qualitative terms
Information security risks

- Replacement costs (software, hardware, other)
- Backup restoration and recovery costs
- Reprocessing, reconstruction costs
- Crime (non-computer, computer)

- Loss of life
- Economic impact and financial loss
- Losses due to fraud, theft, larceny, bribery
- Impact of
  - lost competitive edge
  - lost data
  - lost time
  - lost productivity
  - lost business
- Bankruptcy
- Business interruption
- Frustration
- Ill will
- Injury
- Impacts of inaccurate data
Example of an IT risk model
## Risk analysis with an IT risk model

<table>
<thead>
<tr>
<th>Type</th>
<th>Threat Agent</th>
<th>Can exploit this vulnerability</th>
<th>Resulting in this threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Fire</td>
<td>Lack of fire extinguishers</td>
<td>Facility and computer damage, and possible loss of life</td>
</tr>
<tr>
<td>Physical</td>
<td>Intruder</td>
<td>Lack of security guard</td>
<td>Broken windows and stolen computers and devices</td>
</tr>
<tr>
<td>Technical</td>
<td>Contractor</td>
<td>Lax access control mechanisms</td>
<td>Stolen trade secrets</td>
</tr>
<tr>
<td>Technical</td>
<td>Malware</td>
<td>Lack of antivirus software</td>
<td>Virus infection...</td>
</tr>
<tr>
<td>Technical</td>
<td>Hacker</td>
<td>Unprotected services running on a server</td>
<td>Unauthorized access to confidential information</td>
</tr>
<tr>
<td>Administrative</td>
<td>Employee</td>
<td>Lack of training</td>
<td>Unauthorized distribution of sensitive information</td>
</tr>
<tr>
<td>Administrative</td>
<td>Employee</td>
<td>Lack of auditing</td>
<td>Uncontrolled invalid modifications to decision support data</td>
</tr>
</tbody>
</table>
Process for Assessing IT risk

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 32
How to determine if risk is acceptable?
Quantitative risk assessment – **financial method**

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:
   
   - Single loss expectancy (SLE) = Asset value \( \times \) Exposure factor

   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the **annual rate of occurrence (ARO)**. Simply stated, **how many times is this expected to happen in one year?**

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

   - Annualized loss expectancy (ALE) = Single loss expectancy (SLE) \( \times \) Annualized rate of occurrence (ARO)

   Note: This calculation assumes total loss of an asset. If an asset retains part of its useful value, the SLE should be adjusted by an appropriate amount.
Case analysis Team Problem

Meet in group and determine the Annual Loss Expectance (ALE) for the Dean’s laptop theft
### Annual Loss Expectancy Calculation

<table>
<thead>
<tr>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Monitoring Service (1000 records)</td>
<td>$15,000</td>
</tr>
<tr>
<td>Dean’s Lost Productivity (assume $300,000 salary):</td>
<td></td>
</tr>
<tr>
<td>10 hours restoring data from various sources</td>
<td>$3,000</td>
</tr>
<tr>
<td>10 hours re-doing lost work</td>
<td>$3,000</td>
</tr>
<tr>
<td>Replacement Device</td>
<td>$1,000</td>
</tr>
<tr>
<td>IT investigation</td>
<td>$200</td>
</tr>
<tr>
<td><strong>Single Loss Expectancy</strong></td>
<td><strong>$22,200</strong></td>
</tr>
</tbody>
</table>

**Annualized Rate of Occurrence:** 0.05

**Annual Loss Expectancy:** $1,100

*Note that assumptions of 5% probability and credit monitoring service for 1,000 individuals greatly influence the results...*
Risk Management Techniques

Once threats and risks are identified, each risk can be managed by:

1. Avoidance
2. Acceptance
3. Transfer
4. Mitigation
Risk management decision

Decision:
- Mitigate expected loss of a dean’s laptop through purchase of security countermeasures

Annual Loss Expectancy Calculation
Credit Monitoring Service (1000 records): $15,000
Dean’s Lost Productivity (assume $300,000 salary):
  10 hours restoring data from various sources $3,000
  10 hours re-doing lost work $3,000
Replacement Device: $1,000
IT investigation: $200
Single Loss Expectancy: $22,200

Annualized Rate of Occurrence: 0.05
Annual Loss Expectancy: $1,100

Annual Cost of Countermeasures (per device)
Automatic Backups: $300
Managed Device Service: $100
Annual Cost of Countermeasures: $400
Risk mitigations – Which are physical controls?

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure
- Fences
- Role-based access control
- Segregation of duties
- Redundant data center
- Corporate code of conduct
- Internal audit
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Firewalls
- Change management
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredders
- Secure file wipes
- Secure passwords
- Single sign-on
- Environmental controls (air conditioners, humidifiers)
Risk mitigations – Physical controls

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- **Canine patrols**
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure
- **Fences**
- Role-based access control
- Segregation of duties
- Redundant data center
- Corporate code of conduct
- Internal audit
- **Grounds lighting**
- Intrusion detection software
- **Locked doors and terminals**
- Motion-detection devices
- Network firewalls
- Change management
- Penetration testing
- **Placement of authentication / authorization / database / accounting servers in secure location**
- **Receptionists**
- Residue controls - disintegrator / shredders
- Secure file wipes
- Secure passwords
- Single sign-on
- **Environmental controls (air conditioners, humidifiers)**
Risk mitigations – Technical controls

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- Fences
- Role-based access control
- Segregation of duties

- Redundant data center
- Corporate code of conduct
- Internal audit
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Network firewalls
- Change management
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredder
- Secure file wipes
- Secure passwords (may be organizational too)
- Single sign-on
- Environmental controls (air conditioners, humidifiers)
Risk mitigations – Administrative controls

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- **Code of sanctions against vendors/suppliers/contractors**
- **Color-coded ID badges**
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- Fences
- **Role-based access control**
- **Segregation of duties**
- Redundant data center
- **Corporate code of conduct**
- **Internal audit**
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Firewalls
- **Change management**
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredders
- Secure file wipes
- **Secure passwords (may be technical too)**
- Single sign-on
- Environmental controls (air conditioners, humidifiers)
ISACA’s RiskIT Framework

- ISACA’s Risk IT Framework is useful to guide an organization’s approach to trading IT Risk for IT value.
- Also guides implementing IT governance in enterprises adopting COBIT as their IT governance framework for risk management and control.
- COBIT
  
  Control OBjectives for Information and related Technologies

  _ IT governance framework and supporting toolset enabling managers to bridge the gap between business risks, risk control requirements, and technical issues.
The RiskIT Framework

Groups key activities into three domains

Provides guidance on:

- Key activities within each process,
- Responsibilities for the process,
- Information flows between processes
- Performance management of the process
The Risk IT framework is about trading off IT value with IT risk—in other words... business risk related to the use of IT

• The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk
The RiskIT Framework

**IT risk is business risk**

- Associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise

- Consists of IT-related events and conditions that could potentially impact the business
  - *Can occur with both uncertain frequency and magnitude*
  - *Create challenges in meeting strategic goals and objectives*
U.S. laws and regulations that require businesses to protect data and the computer (IT) systems that process them.

<table>
<thead>
<tr>
<th>Law/Regulation</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Insurance Portability and Accountability (HIPAA)</td>
<td>51.5%</td>
</tr>
<tr>
<td>U.S. state data breach notification law</td>
<td>47.4%</td>
</tr>
<tr>
<td>Sarbanes-Oxley Act (SOX)</td>
<td>42.3%</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard (PCI-DSS)</td>
<td>42.3%</td>
</tr>
<tr>
<td>International privacy or security laws</td>
<td>32.5%</td>
</tr>
<tr>
<td>Federal Information Security Management Act (FISMA)</td>
<td>32.0%</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Act (GLBA)</td>
<td>28.9%</td>
</tr>
<tr>
<td>Health Information Technology for Economic and Clinical HealthAct (HITECH Act)</td>
<td>23.2%</td>
</tr>
<tr>
<td>Payment Card Industry Payment Application Standard</td>
<td>16.0%</td>
</tr>
<tr>
<td>Other</td>
<td>13.9%</td>
</tr>
</tbody>
</table>

How do businesses use the law to protect their information?

3 ways businesses protect intellectual property

- **Copyright law** to protect the specific expression of an idea (not the idea) e.g. computer code so it can be distributed to users without security measures
- **Patent law** to protect novel inventions
- **Trade secret law** to prevent breach of confidentiality and recover damages after a breach

Most valuable corporate data is protected by trade secret law, but to use the law a company must first demonstrate that it complied with 1 basic requirement: “it must show it exercised **reasonable efforts** to prevent the loss”

This is how information security meets the legal needs of business today.
What information needs protection?

✓ Business information
• Critical Infrastructure Information (CII)
• *Personally Identifiable Information (PII)*...
• *Protected Health Information (PHI)*...
Critical National Infrastructure

In 1996, President Clinton signed an Executive Order 13010 identifying infrastructure vulnerable to attack

“Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States”

- Telecommunications
- Electrical power systems
- Gas and oil storage and transport
- Banking and finance
- Transportation
- Water supply systems
- Emergency services
- Continuity of government
Federal Homeland Security Act of 2002 defined...

Critical Infrastructure Information – as data that can be used in either physical or computer-based attack that directly or indirectly

- Affects viability of a facility or critical infrastructure
- Threatens public health or safety
- Harms interstate commerce or the United States
- Violates Federal, State, or local law

Protected System – any physical or computer-based system, information or data, process or procedure that directly or indirectly affects the viability of a facility or critical infrastructure
16 U.S. Critical Infrastructure Sectors

- Transportation
- Water and Wastewater Systems
- Dams
- Emergency Services
- Commercial Facilities
- Nuclear Reactors, Materials, and Waste
- Defense Industrial Base
- Communications
- Energy
- Chemical
- Government Facilities
- Critical Manufacturing
- Healthcare and Public Health
- Information Technology
- Food and Agriculture
- Financial Services
Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!
Transportation sector - example

Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!

Even “Isolated” Legacy Systems Are Vulnerable
14 Year Old Boy Derails Polish Trams, January 2008

- 4 light rail trains derailed, 12 people hurt
- Used modified television remote controller
- Locks disabling switch when vehicle present not installed
16 U.S. Critical Infrastructure Sectors

- Transportation
- Commercial Facilities
- Energy
- Healthcare and Public Health
- Water and Wastewater Systems
- Nuclear Reactors, Materials, and Waste
- Chemical
- Information Technology
- Dams
- Defense Industrial Base
- Government Facilities
- Food and Agriculture
- Emergency Services
- Communications
- Critical Manufacturing
- Financial Services
Vitek Boden worked for Hunter Watertech, an Australian firm that installed SCADA radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia (a rural area of great natural beauty and a tourist destination)

- Applied for a job with the Maroochy Shire Council
- Walked away from a “strained relationship” with Hunter Watertech
- The Council decided not to hire him
- Boden decided to get even with both the Council and his former employer

• **Maroochy Shire Council had no existing information security policies, procedures, nor cyber security defenses**

• On at least 46 occasions Boden issued radio commands to the sewage equipment
  - Caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel
  - Marine life died, the creek water turned black, the stench was unbearable for residents
The Water and Wastewater Systems Sector is vulnerable to:

- Natural disasters
- A variety of attacks, including:
  - Contamination with deadly agents
  - Physical attacks (such as the release of toxic gaseous chemicals)
  - Cyberattacks

Denial of service in Water and Wastewater System Sector would impact:

- Critical services: firefighting and healthcare (hospitals),
- Other sectors: Energy, Food and Agriculture, and Transportation Systems

~153,000 public drinking water systems
>80% of U.S. population receives their potable water from these drinking water systems

>16,000 publicly owned wastewater treatment systems
~75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems


Attack impacts:
- Large numbers of illnesses or casualties

Denial of service impacts:
- Public health
- Economic vitality
ISO/IEC 27001 Standard

Considered the leading example of risk management for information security

– Created in 2005 and updated in 2013 by agreement between
  • International Organization for Standardization (ISO)
  • International Electro-technical Commission (IEC)
– Specific requirements for security management systems and controls
– Firms can apply to be audited and certified as ISO/IEC 27001 compliant
Federal Information Security Management Act of 2002
Federal Information Security Modernization Act of 2014

Recognize importance of information security to U.S. economy and national security
• Require each federal agency to provide information security
  – For information and information systems supporting their operations and assets
    – Including those provided or managed by another agency, contractors, or other source

https://www.dhs.gov/fisma
FISMA - Federal Information Security Management Act defines “Information security” as protection of...

- Confidentiality, integrity, and availability (“CIA”) of data and information
- Data, information and information systems from unauthorized...

- Access, use, disclosure = Confidentiality
- Modification = Integrity
- Disruption or destruction = Availability
What is NIST?

– Non-regulatory agency of the United States Department of Commerce
– Measurement standards laboratory

Mission: *Promote innovation and industrial competitiveness*

• NIST's activities organized as laboratory programs:
  – Nanoscale Science and Technology, Engineering, Neutron Research, Material Measurement, Physical Measurement...
  – Information Technology

_NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets (excluding national security systems)_
RISK MANAGEMENT FRAMEWORK (RMF) OVERVIEW

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of organizational risk—that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization.

Risk-Based Approach

The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. The following activities related to managing organizational risk (also known as the Risk Management Framework) are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture.

Step 1: Categorize

Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.\(^1\)

Step 2: Select

Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions.\(^2\)

Step 3: Implement

Implement the security controls and document how the controls are deployed within the information system and environment of operation.

\(^1\) Impact analysis is the process of identifying and assigning values to risks that may result from threats to an information system. Impact analysis is typically performed to identify the level of protection needed for an information system.

\(^2\) Organization assessment of risk is the process of identifying and analyzing risks to an information system.
MIS 5206 Protecting Information Assets
TIER 1
ORGANIZATION (Governance)

TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
NIST Cybersecurity Framework

Refers to and builds on many principles of the ISO/IEC 27001 standard (and others)

Goes way beyond IT and physical security environment
...by also including:
• Governance and management
• Staff policies and procedures
• Training
• Supply chain management
### NIST Cybersecurity Framework’s Core Functions

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>What assets need protection?</td>
<td>IDENTIFY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What safeguards are available?</td>
<td>PROTECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What techniques can identify</td>
<td>DETECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>incidents?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What techniques can contain</td>
<td>RESPOND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>impacts of incidents?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What techniques can restore</td>
<td>RECOVER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>capabilities?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functions</td>
<td>Categories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>PR.IP</td>
<td>Information Protection</td>
</tr>
<tr>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>DE.CM</td>
<td>Security Continuous</td>
</tr>
<tr>
<td></td>
<td>DE.DP</td>
<td>Monitoring</td>
</tr>
<tr>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
## Cybersecurity Framework’s Capability Maturity Tiers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partial</strong></td>
<td>Not formalized</td>
<td>Limited awareness</td>
<td>No external collaboration</td>
</tr>
<tr>
<td></td>
<td>Reactive</td>
<td>Irregular risk management</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Informed</strong></td>
<td>Approved practices</td>
<td>More awareness</td>
<td>Not formalized to interact &amp; share information</td>
</tr>
<tr>
<td></td>
<td>Not widely use as policy</td>
<td>Risk-informed, processes &amp; procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adequate resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal sharing</td>
<td></td>
</tr>
<tr>
<td><strong>Repeateable</strong></td>
<td>Approved as Policy</td>
<td>Organization approach</td>
<td>Collaborate</td>
</tr>
<tr>
<td></td>
<td>Update regularly</td>
<td>Risk-informed, processes &amp; procedures defined &amp; implemented as intended, and reviewed</td>
<td>Receive information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Knowledge &amp; skills</td>
<td></td>
</tr>
<tr>
<td><strong>Adaptive</strong></td>
<td>Continuous improvement</td>
<td>Risk-informed, processes &amp; procedures for potential events</td>
<td>Actively shares information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Continuous awareness</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Actively</td>
<td></td>
</tr>
</tbody>
</table>
In summary...

The RiskIT Framework

NIST Critical Infrastructure Cyber Security Framework

NIST Risk Management Framework
How do you analyze risk when the need for InfoSec is measured in terms of life-safety and not financial risk measures?

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Preservation of information, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</td>
<td>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</td>
<td>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</td>
<td>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>
Test Taking Tip

- Read the answers first -

This contradicts many people’s test taking recommendations...

...but, it works. Here’s why:

• Quickly alerts you to the type of question to expect

• Focuses your attention in reading the question for meaningful information

• Gives you advanced warning that there may be more than one significant concepts (option to answer in the form “Both A & B”)

• Gives you an opportunity to get a sense of the sort of answer the test maker is looking for

• There may be more than one valid answer, but the test maker may be looking for “best mitigation for the situation” or “least risk in the situation”
Example:

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A
Example:

Which of the following represents the GREATEST potential risk in an Electronic Data Interchange (EDI) environment?

A. Transaction authorization  
B. Loss or duplication of EDI transmissions  
C. Transmission delay  
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A
Example:

Which of the following represents the GREATEST potential risk in an Electronic Data Interchange (EDI) environment?

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A
1. Which of the choices below is the most often used criteria to determine the classification of a business object?
   a. Value
   b. Useful life
   c. Age
   d. Personal association

2. Which of the below definitions is the best description of a vulnerability?
   a. A weakness in a system that could be exploited
   b. A company resource that is lost due to an incident
   c. The minimum loss associated with an incident
   d. A potential incident that could cause harm

3. Which statement below best describes the purpose of risk analysis?
   a. To develop a clear cost-to-value ratio for implementing security controls
   b. To influence the system design process
   c. To influence site selection decisions
   d. To quantify the impact of potential threats

4. What is an ARO?
   a. A dollar figure assigned to a single event
   b. The annual expected financial loss to an organization from a threat
   c. A number that represents the estimated frequency of an expected event
   d. The percentage of loss that would be realized for a specific asset if a threat occurred

5. Which group represents the most likely source of an asset loss through in appropriate computer use?
   a. Crackers
   b. Hackers
   c. Employees
   d. Saboteurs
Quiz – Week 2

1. Which of the choices below is the most often used criteria to determine the classification of a business object?

   a. Value
   b. Useful life
   c. Age
   d. Personal association
1. Which of the choices below is the most often used criteria to determine the classification of a business object?

a. Value
b. Useful life
c. Age
d. Personal association
2. Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm
Quiz – Week 2

2. Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited  
b. A company resource that is lost due to an incident  
c. The minimum loss associated with an incident  
d. A potential incident that could cause harm
3. Which statement below best describes the purpose of risk analysis?

a. To develop a clear cost-to-value ratio for implementing security controls
b. To influence the system design process
c. To influence site selection decisions
d. To quantify the impact of potential threats
3. Which statement below best describes the purpose of risk analysis?

a. To develop a clear cost-to-value ration for implementing security controls
b. To influence the system design process
c. To influence site selection decisions
d. To quantify the impact of potential threats
4. What is an ARO?

a. A dollar figure assigned to a single event
b. The annual expected financial loss to an organization from a threat
c. A number that represents the estimated frequency of an expected event
d. The percentage of loss that would be realized for a specific asset if a threat occurred
Quiz – Week 2

4. What is an ARO?

a. A dollar figure assigned to a single event
b. The annual expected financial loss to an organization from a threat

Correct: c. A number that represents the estimated frequency of an expected event

d. The percentage of loss that would be realized for a specific asset if a threat occurred

MIS 5206 Protecting Information Assets
5. Which group represents the most likely source of an asset loss through inappropriate computer use?

a. Crackers  
b. Hackers  
c. Employees  
d. Saboteurs
5. Which group represents the most likely source of an asset loss through inappropriate computer use?

a. Crackers
b. Hackers
c. Employees
d. Saboteurs
Next week’s reading questions

• What are the 3 types of risk mitigating controls? Which is the most important? Why is it the most important?
• How you would apply the FIPS security categorizations to decide if each of the information security risk mitigations ("safeguards") described in the FGDC guidelines is needed?
• Which two information security objectives could be put at risk if the alternative mitigations (i.e. "safeguards") recommended by the FGDC guidelines are applied? Explain how each could be put at risk.
MIS5206 Week 2

- In the News
- Readings
- Understanding an Organization’s Risk Environment
- Test Taking Tip
- Quiz
- Next week
Protecting Information Assets
- Week 2 -

Understanding an Organization’s Risk Environment