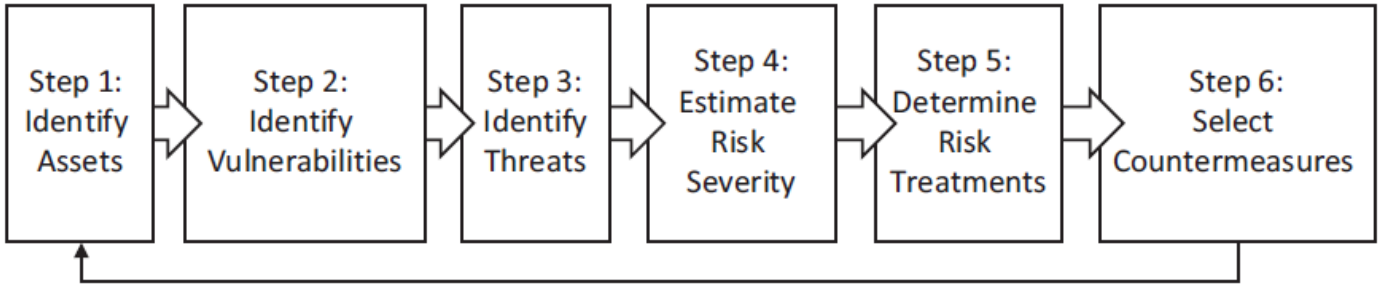
Lecture 4

Security Management and Risk Assessment

Cyber Risk Management

- Cyber risk management is a systematic process for analyzing how an organization could succumb to cyberattacks, and explores options for reducing either the likelihood or the impact of the attacks that occur.
- Cyber risk analysis involves performing an integrated set of activities, according to a risk management process, to identify potential security compromises, their consequences, and ways to mitigate them.
- While there are a number of risk management processes, they generally involve performing these steps:



Cyber Risk Management Process

- The risk management process identifies assets, vulnerabilities, threats, risks, risk severity, associated risk treatments, and countermeasures. Risk severity is measured in terms of risk likelihood and risk impact. These key terms are defined as follows:
  - Assets are anything of value to an organization or to attackers. For example, social security numbers, computers, and servers are all assets, along with customer databases and proprietary intellectual property.
  - Vulnerabilities are weaknesses that attackers may exploit to harm one or more assets that an organization cares about. For example, computer operating systems may have vulnerabilities due to missing software updates or patches, or web sites may have vulnerabilities in their underlying code.
  - Threats are the ways attackers exploit vulnerabilities to cause damage to organizational assets. For example, one type of threat is computer viruses infecting organizational computers due to missing software updates or patches.

Cyber Risk Management Process

- Risk is the potential damage to assets, causing an impact to the organization. For example, a risk can be when attackers use compromised computers to steal data, embezzle money, or take critical systems off line.
- Risk likelihood refers to the likelihood that the risk will manifest itself, resulting in a consequence. For example, likelihood could be characterized in terms of low likelihood (unlikely to occur), medium likelihood (possible to occur), or high likelihood (likely to occur).
- Risk impact refers to how great the consequence of the risk is to the organization's business and priorities. For example, the risk could have a low impact (a slight effect), a medium impact (a moderate effect), or a high impact (a significant effect).

Cyber Risk Management Process

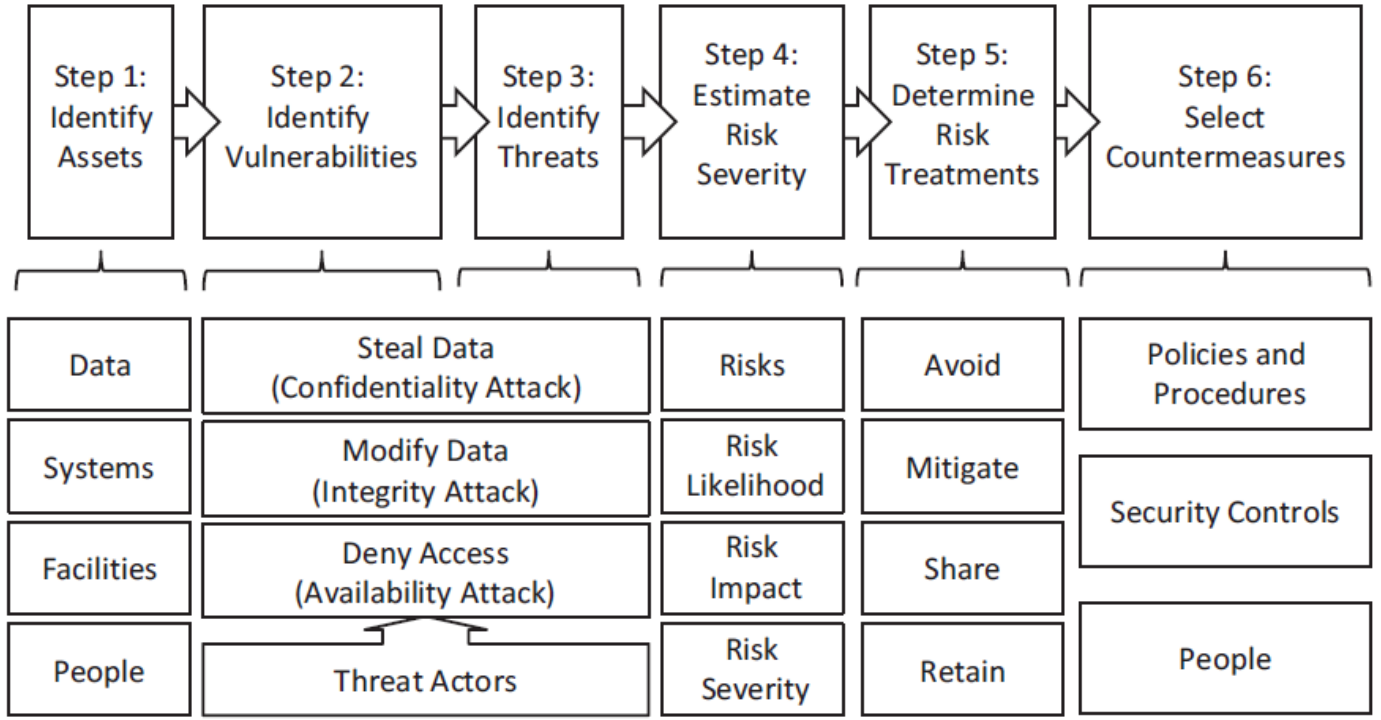
- Risk severity is determined by combining the risk likelihood and risk impact of each potential threat into an "overall" risk level – a risk severity level. This risk severity level can then be used to prioritize risks and consider potential risk treatments. For example, a risk that is characterized as being low risk (unlikely to occur), but having a high impact (significant effect) on the organization might be assigned an overall risk severity level of "medium."
- Risk treatments are ways to reduce risk besides just trying to prevent the risk from happening. For example, an organization can "avoid" the risk by eliminating the vulnerability or threat, or it can "reduce the likelihood" of the risk manifesting itself through cyberdefenses, or it can "reduce the impact" by purchasing cyber insurance.
- Countermeasures are security protections designed to reduce risk by eliminating vulnerabilities or countering potential threats. For example, an organization can implement cybersecurity controls to "reduce the likelihood" that the risk will occur by blocking potential cyberattacker activities.

Cyber Risk Management Process

- Security professionals perform the cyber risk management process within the context of applicable cybersecurity drivers that include the following: (1) laws and regulations, (2) cybersecurity standards, (3) contractual obligations, and (4) liability and insurance.
- Security professionals should be interested in identifying and addressing the most pressing organizational risks, while understanding that risk can be reduced but seldom eliminated.
- Risk management involves balancing factors of cost, convenience, and speed to find ways to reduce risk without getting in the way of the organization too much. Remember, there is no perfect cyberdefense.

Cyber Risk Management Process

- The figure below shows additional details for the six-step cyber risk management process:



Cyber Risk Management Process

- Step 1: Identify Assets
  - The first step in the cyber risk management process identifies and inventories the assets that are of value to the organization and should be protected.
  - Assets can include the following:
    - Data is the information held by the organization, whether it is proprietary, customer, organizational, vendor, or personal data.
    - Systems use processes, procedures, and data to accomplish organizational or personal goals.
    - Facilities are the locations where people in the organization work, or a person or family resides, and the tools and equipment at those locations.
    - People are the organization's personnel, partners, or family members, along with their knowledge and abilities.

Cyber Risk Management Process

- Step 2: Identify Vulnerabilities
  - The second step in the cyber risk management process identifies vulnerabilities that could be exploited by threats or threat actors to harm the assets that organizations care about.
  - A useful technique in identifying vulnerabilities is to consider consequences that may occur when a vulnerability has been exploited, or when a protection fails or is missing.
  - Cyberattacks have several major goals that include the following:
    - Confidentiality attacks seek to steal data that is valuable and should be kept confidential.
    - Integrity attacks seek to modify data to cause disruption or harm.
    - Availability attacks seek to deny access to systems, services, or data by making them unavailable to the people who need them.

Cyber Risk Management Process

- Vulnerability analysis involves considering situations where something occurs that makes the chance of a threat manifesting itself greater than “normal.”
- Vulnerability might be present when a door that is normally locked is left unlocked, or a sensitive computer is connected to a public network, or third parties are allowed into our homes or offices.
- An organization will want to apply these types of mindsets to its IT systems, to identify vulnerabilities related to how systems operate, how they interact, and how they interconnect.
- A vulnerability increases the likelihood that something bad might happen.

Cyber Risk Management Process

- Step 3: Identify Threats
  - The third step in the cyber risk management process identifies the threats that may jeopardize organizational assets.
  - Threats frequently revolve around threat actors who may wish to do us harm. Threats may be natural or man-made, accidental or deliberate, random, or deterministic.
  - Examples of threat actors and threats that an organization may want to consider include the following:
    - Carelessness that includes mistakes and negligence, that can cause security to be compromised, data to be exposed, or systems to be disabled.
    - Commodity threats that include random malware, viruses, worms, and botnets. Commodity threats may exploit vulnerabilities or other cyberdefense weaknesses, but they do not usually adjust or adapt to work their way around protections that are in place.

Cyber Risk Management Process

- Competitors looking to steal business or gain an advantage.
- Customers with whom organizational relationships are not always good.
- Cybercriminals have found that there is serious money to be made on the internet.
- Cyberterrorism is conducted using similar techniques as cybercrime, but by unaffiliated individuals or terrorist organizations.
- Cyberwar is about damaging the ability of organizations or governments to operate in cyberspace.
- Espionage takes cybercrime to the next level, but is generally focused on stealing information.
- Hackers who want to control organization computers or accounts, and then exploit that control to serve their personal or organizational objectives.
- Hacktivists conducting targeted attacks to make a public or political statement.
- Insiders who may be employees or trusted third parties who want to steal from or sell out the organization.
- Nature should never be underestimated as it can destroy facilities, disable personnel, and disrupt operations.

Cyber Risk Management Process

- Step 4: Estimate Risk Severity
  - When estimating risk severity, it is helpful to start the process by constructing risk statements using the assets, vulnerabilities, and threats that were identified in the preceding three steps, along with a corresponding consequence that the organization cares about.
  - The following sentences are examples of potential day-to-day risk statements:
    - A criminal steals your driver's license and credit card because you left them lying out, causing you inconvenience.
    - A rainstorm leaks through a broken window, causing water damage to office computers.
    - An employee inadvertently posts customer data to a public website, resulting in a breach of confidential personal information.
    - Customers get away with shoplifting merchandise because of poor inventory management, costing the business money.
    - Ransomware installs itself on your unpatched internet-connected computer, destroying your valuable photos and documents.

Cyber Risk Management Process

- Each of these risk statements identifies a risk in terms of assets, vulnerabilities, threats, and consequences:
  - Assets include credit cards, computer data, confidential customer information, merchandise, and office computers.
  - Threats include criminals, hackers (ransomware), careless employees, customers, and acts of nature.
  - Vulnerabilities include leaving things lying around, missing patches, poor data protection, poor inventory management, and broken windows.
  - Consequences include inconvenience, loss of valuable data, breach of confidential data, loss of revenue, or property damage.

Cyber Risk Management Process

- Once risk statements have been constructed, the risks themselves can then be considered in terms of two properties: likelihood and impact.
  - Likelihood refers to how likely it is that the risk will manifest itself, resulting in a consequence.
  - Impact refers to how great the consequence of the risk is, in the grand scheme of things
  - The following figure illustrates one way in which risk likelihood and risk impact can be combined into an overall risk level or risk severity.

		Risk Impact		
		Low (Risk has *slight* effect)	**Medium** (Risk has *moderate* effect)	**High** (Risk has *significant* effect)
Risk Likelihood	**High** (Risk *likely* to occur)	**Medium**	**High**	**High**
	Medium (Risk *possible* to occur)	**Low**	**Medium**	**High**
	Low (Risk *unlikely* to occur)	**Low**	**Low**	**Medium**

Cyber Risk Management Process

- Likelihood and impact can both be analyzed to
  - (1) understand how great the risk really is,
  - (2) group risks by their relative severity, and
  - (3) provide input to budgetary and investment decisions.
- Security and IT professionals, among others, can provide their “expert judgment” regarding risk likelihood and risk impact, as follows:
  - Low severity risks might be those risks with a low likelihood and a low impact. Low severity risks are often categorized as a low-priority budget investment, and frequently may be accepted, without mitigation.
  - Medium severity risks might be those risks with a high likelihood and a low impact, or a low likelihood but a high impact. Medium severity risks often require further analysis to understand the risks so that management can decide what needs to be done to mitigate them.
  - High severity risks might be those risks with a high likelihood, and a high impact. High severity risks should be given priority for mitigation and have their severity reduced through treatments or countermeasures.

Cyber Risk Management Process

- Step 5: Determine Risk Treatments
  - Not all risks can be mitigated, especially when cost is a consideration.
  - Similarly, even risks that can be significantly reduced can seldom be eliminated completely.
  - For example, some risks may have to be accepted as a “cost of doing business,” such as the chance of occasional shoplifting when operating a convenience store.
  - Other risks, like natural disasters or acts of war, are simply far outside an organization’s ability to control in any way.

Cyber Risk Management Process

- However, organizations can reduce risk by using the following risk treatments:
  - Avoid the risk by eliminating the vulnerability or the threat.
  - Mitigate the risk by reducing the likelihood that it will occur or the impact when it does occur.
  - Share the risk by introducing a third party (such as an insurance company or a security service) that compensates the organization in the event that the risk occurs.
  - Retain the risk, where the organization simply accepts the possibility that the risk may occur and deals with the consequences when it happens; self-insurance is a good example of this strategy

Cyber Risk Management Process

- Step 6: Select Countermeasures
  - Countermeasures can include security policies and procedures, security controls, and people.

  - Countermeasure Policies and Procedures
    - Countermeasure policies and procedures define required organization cybersecurity behavior.
    - Policies define what is to be protected and to what degree, along with organizational responsibilities.
    - For example, a countermeasure policy may require data in motion or data at rest to be encrypted.

Cyber Risk Management Process

- Security Controls
  - Security controls2 are applied to an IT system or business process to prevent, detect, or investigate specific activities that are undesirable, and respond to those activities when they occur.
  - Security controls can reduce risk by preventing and detecting bad behavior, or helping to seek out and investigate when something bad has occurred.
  - Security controls include the following types:
    - Preventive controls. Block undesired activities and prevent them from occurring.
    - Detective controls. Generate alerts on suspected attacker activity that can then be acted upon.
    - Response controls. Activated after detective controls “alert” cyber personnel of suspected attacker activities, and assist defenders in investigating the alert, identifying the cyberattack, containing the attacker, and ultimately repelling the attack.
    - Recovery controls. Engaged to close out cyber incidents and restore normal operations.

Cyber Risk Management Process

- People
  - People involved with security countermeasures include employees, partners, and contractors authorized to have specific access to organizational assets.
  - Authorized employees include executives, IT staff, and security staff. Security and IT professionals should have the knowledge, skills, abilities and industry-accepted certifications required to carry out their day-to-day security responsibilities.
  - Similar comments can be made regarding contractors, third party organizations, or subject matter experts hired to support an organization's cybersecurity program.
  - An organization's actual security against a professional attacker is almost entirely dependent on its people, not its technology.

Cyber Risk Management Process

- Security controls can have the following capabilities:
  - Reduce likelihood - Controls can reduce how likely it is for the risk to occur, or can make it more difficult for attackers to execute on the risk.
  - Reduce impact - Controls can reduce the impact when the risk does occur, perhaps by limiting the amount of damage that occurs.
  - Detect occurrence - Controls can detect the occurrence of the risk happening, allowing for an active response to thwart the attack, contain the damage, and reduce the potential exposure.
  - Collect evidence - Controls can collect evidence that is used to show the operation of security controls, detect failures of the controls, or support investigations after an incident has occurred.

Risk Registers

- Organizations can use a risk register to document and track identified risks, along with their associated mitigations.
- At this point in the cyber risk management process, a systematic security analysis has identified assets, vulnerabilities, and threats.
- Risks have been identified and evaluated, and corresponding risk treatments have been determined.
- Security countermeasures have been selected and now need to be implemented.
- The risk register acts as a repository for tracking and managing these identified risks. Such registers can be implemented using a spreadsheet, database, or dedicated risk management software package.

Risk Registers

- A risk register frequently contains data fields to include the following:
  - Risk identification number uniquely identifies the risk.
  - Description of the risk briefly characterizes the nature of the risk.
  - Risk likelihood refers to how likely it is that the risk will manifest itself, resulting in a consequence.
  - Risk impact refers to how great the consequence of the risk is, in the grand scheme of things.
  - Risk severity based on an analysis of risk likelihood and risk impact.
  - Risk treatments identifying if the risk is to be avoided, mitigated, shared, or retained.
  - Countermeasures consisting of policies, procedures, security controls, and people.
  - Risk owner who is the individual responsible for ensuring countermeasures are implemented for the identified risk.
  - Status indicating the progress of the selected risk treatment for the identified risk.