TOWSON UNIVERSITY

Risk Management

Dr. Atul Rawal

Risk Management

TOWSON UNIVERSITY

The identification, assessment, and prioritization of risks

- Identify, characterize threats
- Assess the vulnerability of critical assets to specific threats
- Determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
- Identify ways to reduce those risks
- Prioritize risk reduction measures based on a strategy

Risk management does NOT eliminate risks.
Not all risks are created equal or should be treated the same.
Cannot focus on cyber security risks in a silo to be effective.
Goal – identify the risks, determine the appropriate actions.

What is at Risk?

Networks – is someone on the network, capturing the data?

Data – is it being taken or altered?

What is risk with respect to information systems?

TOWSON UNIVERSITY

- Potential harm that may arise from some current process or future event
- Process of understanding and responding to factors that may lead to failure in confidentiality, integrity, and availability of a system/data
- Likelihood
- Threat
- Vulnerability
- impact

Overview of Risk Management

TOWSON UNIVERSITY

- Know yourself: identify, examine, and understand the information and systems currently in place.
- Know the enemy: identify, examine, and understand threats facing the organization.
- Risk management does NOT eliminate risks.
- Not all risks are created equal or should be treated the same.
- Goal – identify the risks, determine the appropriate actions.

What We Know About Risk

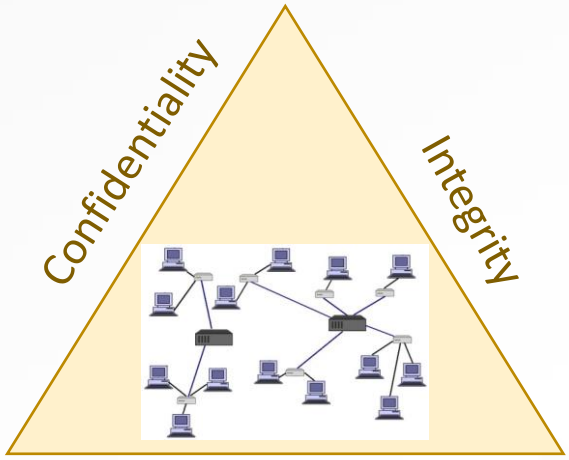
- The possibility of loss or injury.
- The chance an unwanted event occurs.
- Uncertain – likelihood can only be estimate.
- Requires human interpretation and value judgments specific to a situation.

Not all risk is bad, some level of risk must be taken in order to progress / prevent stagnation

Cyber Security Risk – **KEY Components**

- Confidentiality – preventing unauthorized disclosure of information.
- Integrity – ensure not modified or destroyed.
- Availability – available when needed.

Threats can compromise the confidentiality, integrity and/or availability of information processed, stored or transmitted by IT systems.



RISK Components

TOWSON UNIVERSITY

- Losses occur when a threat exposes a vulnerability
- **Loss** – results in a compromise to business functions or assets that adversely affects the business
  - Compromise of business functions – activities a business performs, can result in a loss of revenue
  - Compromise of business assets – anything of measurable value, tangible and intangible
  - Driver of business costs

EXAMPLE – a HACKER

Risk Identification

- **Risk** is the likelihood that a loss will occur.
- Losses occur when a threat exposes a vulnerability
- **Threat** – any activity that represents a possible danger
- **Vulnerability** -

- To Identify Risks:
  1. Identify threats
  2. Identify vulnerabilities
  3. Estimate the likelihood of a threat exploiting a vulnerability

Example: a Microsoft patch is not applied

Vulnerability = what the patch was fixing

Threat = someone may gain access to a network or data if the patch is not applied

Likelihood= ??

Consider ---

- Confidentiality
  - Data at rest
  - Data in transmission
  - All data equal with requirements?
- Integrity
  - Versioning
  - Change management
- Availability
  - Backups (onsite and offsite)
  - Required hours of operation

Risk Management Process

TOWSON UNIVERSITY

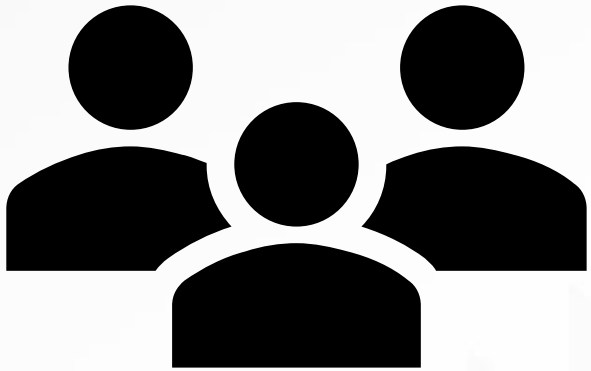
1. Asset identification
2. Identify Threats
3. Identify Vulnerabilities
4. Assess Risks
5. Determine Countermeasures

Step #1 - Asset Identification and Valuation

1. People
2. Data and Information
3. Procedures
4. Software
5. Hardware

People

- Asset attributes for people:
  - Position name/number/ID;
  - Supervisor;
  - Security clearance level;
  - Special skills



Procedures

- IT and business standard procedures
- IT and business sensitive procedures
- Asset attributes for procedures:
  - Description
  - Intended purpose
  - What elements is it tied to
  - Storage location for reference
  - Storage location for update

Data

TOWSON UNIVERSITY

- Asset attributes for data:
  - Owner/creator/manager
  - Data structure size; data structure used
  - Online/offline; location
  - Backup procedures employed
  - Classification scheme

Hardware, Software, and Network Asset Identification

TOWSON UNIVERSITY

- Asset attributes to be considered are:
  - Name
  - IP address
  - MAC address
  - element type
  - serial number
  - manufacturer name
  - model/part number
  - software version
  - physical or logical location
  - controlling entity

Asset Identification and Inventory

TOWSON UNIVERSITY

- Iterative process; begins with identification of assets, including all elements of an organization's system (people, procedures, data and information, software, hardware, networking)
- Assets are then classified and categorized

Mission Critical Systems

TOWSON UNIVERSITY

- What are mission critical systems, application and data
  - Any system or application that must continue to run to ensure business runs
  - Critical Business function – vital to an organization, if fails, cannot perform essential operations = monetary loss
- Relates to Company mission and goal and how the system is used
  - Internet access?
  - Web server availability?
  - Data base server?
- What are the legal and compliance requirements?

Information Asset Valuation

TOWSON UNIVERSITY

Questions help develop criteria for asset valuation: which information asset.

- Is most critical to organization's success?
- Generates the most revenue/profitability?
- Would be most expensive to replace or protect?
- Would be the most embarrassing or cause greatest liability if revealed?

Risk Management scope

TOWSON UNIVERSITY

- Identify critical business operations
  - Identify costs, direct and indirect for an outage, data loss, etc.
- Services provided to customers – expectations ??
  - Internal and external customers
  - Email services
  - Access to internet
  - Access to networks, and applications
  - Access to file servers
  - Customer support (by application and usage)

Information Asset Valuation

TOWSON UNIVERSITY

- Critical – compromise to assets would have grave consequences leading to loss of life, serious injury, or mission failure. (50-100)
- High – compromise to assets would have serious consequences that could impair operations for a significant period of time. (13-50)
- Medium - compromise to assets would have moderate consequences that could impair operations for a limited period of time. (3-13)
- Low - compromise to assets would have little or no impact on the continuation of operations. (1-3)

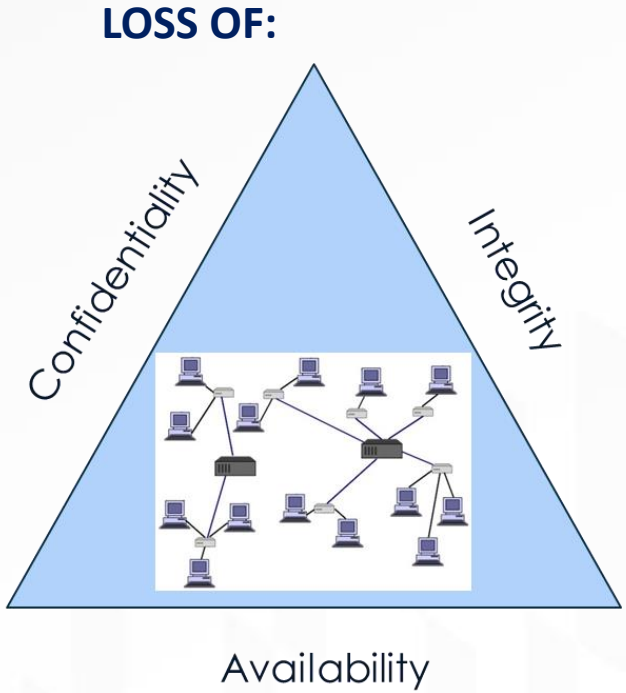
Step #2 Threat Identification

TOWSON UNIVERSITY

- Realistic threats need investigation; unimportant threats are set aside.
- Threat assessment:
  - Which threats present danger to assets?
  - Which threats represent the most danger to information?
  - How much would it cost to recover from attack?
  - Which threat requires greatest expenditure to prevent?

Identify the threats

- Threat = any activity that represents a possible danger or loss.
- Identify the threats
  - Internal / external
  - Natural or man-made
  - Intentional or accidental
- Use the vulnerabilities as a source.



Threat

TOWSON UNIVERSITY

- A possible danger that might exploit a vulnerability to breach security and thus cause possible harm.
- A threat can be either “intentional” (i.e., intelligent; e.g., an individual cracker or a criminal organization) or “accidental" (e.g., a computer malfunction, environmental such as an earthquake, or fire) or otherwise a circumstance, capability, action, or event.
- Threats take advantage of your vulnerabilities.

Threat categories

TOWSON UNIVERSITY

- Human Threats
  - Internal
    - Current or past employees
    - Intentional or unintentional
  - External
    - Hackers
    - Intentional or unintentional
    - Malware, denial of service, terrorists
- Natural Threats

“New” Threats

TOWSON UNIVERSITY

- **Bring your own device (BYOD)** - the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged company information and applications.

- **Cloud computing** - the use of computing resources (hardware and software) which are available in a remote location and accessible over a network (typically the internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software, and computation.

- **Big data** - collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications.

26

Threat Assessments

TOWSON UNIVERSITY

- Identifies and evaluates potential threats
- Identify as many possible threats as possible
- List will not be complete
- Identify most likely threats
- Estimate frequency
- Performed at a specific time
- Evaluates current threats in an existing environment

Threat assessment Best Practices

TOWSON UNIVERSITY

- **Assume nothing- you don't know what you don't know.**
- Things change.
- Verify system operates as expected.
- Limit scope to single domain at a time.
- Use documentation and diagrams to understand.
- Identify all entry points.
- Consider threats to confidentiality, integrity and availability.
- Consider internal and external human threats.
- Consider natural threats.

Identifying threats:

TOWSON UNIVERSITY

- Review historical data.
- Specific information on past threats.
  - Organization
    - Internal users
    - Disgruntled employee
    - Equipment failure
    - Software failure
    - Data loss
    - Attacks
  - Similar organizations
  - Local area (natural events)
- No guaranteed threats will be repeated.
- No guarantee new threat won't appear.

Threat Identification

TOWSON UNIVERSITY

THINK OUTSIDE THE BOX

THINK LIKE AN ATTACKER

Step #3 Vulnerability Identification

TOWSON UNIVERSITY

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities.
- Examine how each threat could be perpetrated and list organization's assets and vulnerabilities.
- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions.
- At end of risk identification process, list of assets and their vulnerabilities is achieved.

Step #3 Vulnerability Identification

- Human
- Operational – insufficient security procedures
- Informational vulnerabilities
- Facility – weak physical location and geographical
- Equipment

Identify the Vulnerabilities

Vulnerability - weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.

- Vulnerability = Weakness
- Where are Vulnerabilities?
- Sources for Identification
- Audits
- Certification and accreditation (ATO, OSA)
- System logs, scan reports
- Incident response investigations
- Use ALL IT Domains
  - User – people
  - Workstation – end user's computer
  - Networks(LAN & WAN)
  - Remote Access

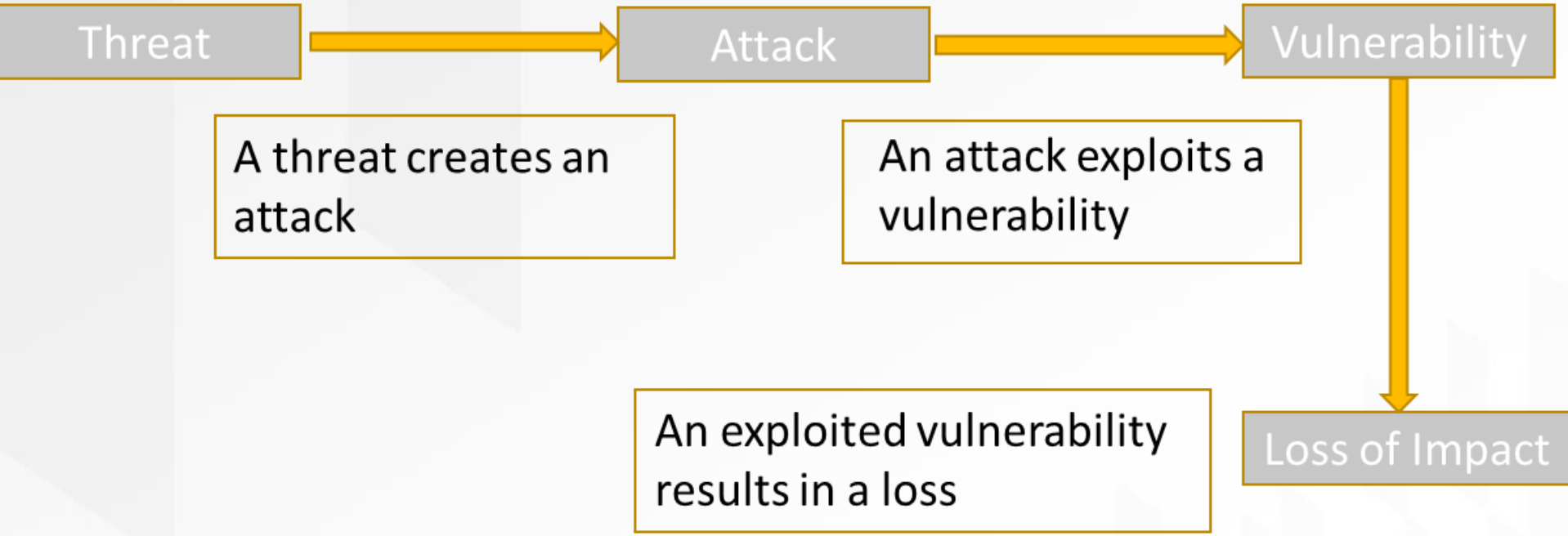
Vulnerability Valuation

TOWSON UNIVERSITY

- Critical – no known countermeasures and adversary capability exists. (75%-100%)
- High –some countermeasures, multiple weaknesses exist that adversaries could exploit. (50%-74%)
- Medium – there are effective countermeasures in place, but adversaries can exploit a weakness. (25%-49%)
- Low - multiple levels of countermeasures exist and few or no adversaries could exploit the asset. (0%-24%)

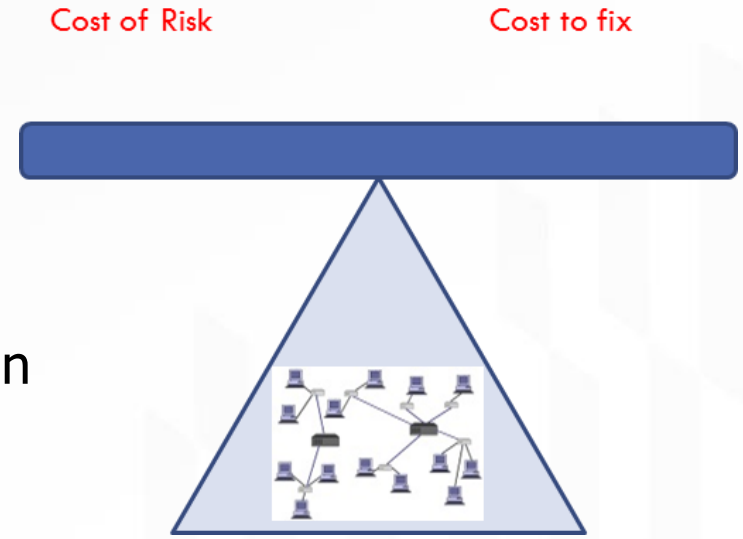
Threats and Vulnerabilities

TOWSON UNIVERSITY



Risk Appetite

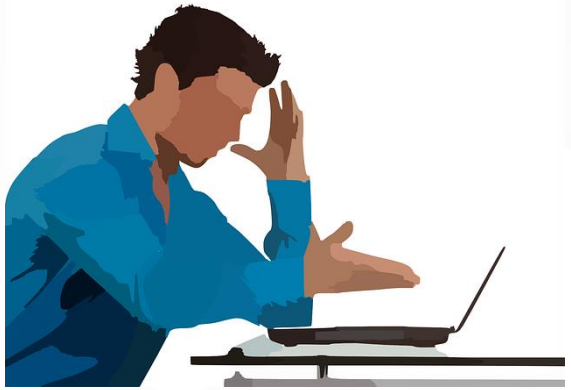
- The amount of risk an organization is willing to accept in pursuit of its objectives given consideration of costs and benefits.
- Provides guidance on the amount of risk that is acceptable in pursuit of objectives.
- Help make informed decisions.
- Decisions with regard to:
  - Allocation of resources
  - Management controls
  - Potential consequences
  - Impacts to other parts of organization



Residual risk

- The risk that remains

- Residual risk = total risk - controls



Risk Assessment

TOWSON UNIVERSITY

- Risk assessment evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each information asset
- The goal at this point: create a method for evaluating the relative risk of each listed vulnerability

Probability/Likelihood

TOWSON UNIVERSITY

- The probability that a specific vulnerability will be the object of a successful attack
- Assign numeric value: number between 0.1 (low) and 1.0 (high), or a number between 1 and 100
- Zero not used since vulnerabilities with zero likelihood are removed from asset/vulnerability list
- Use selected rating model consistently
- Use external references for values that have been reviewed/adjusted for your circumstances

Risk Profile

- Risk profile – listing and assessment of the business's top risks
- Purpose –
  - provide a thoughtful analysis of the risks an organization is facing towards achieving its strategic objectives and arising from activities and operations.
  - identify those risks which significantly impact FSA from achieving its strategic objectives, as well as any other noteworthy, but non-strategic, risks
- Assists in facilitating a determination around the aggregate level and types of risks that an organization and its management are willing to assume

Types of risk assessments

TOWSON UNIVERSITY

Quantitative

- Objective method
- Uses numbers such as actual dollar values
- Math problem with formulas
- Requires significant amount of data that can take time to gather

Qualitative

- Subjective method
- Use relative values based on opinions from experts
- Uses words such as Low, Moderate, High
- Uses probability and impact

Documenting the Results of Risk Assessment

TOWSON UNIVERSITY

- Final summary comprised in ranked vulnerability risk worksheet
- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor
- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk

Risk Mitigation Plan

- Risk assessment complete and approved
  - Cost Benefit Analyses completed
  - Countermeasures approved

- Risk Mitigation Plan
  - Identify costs
  - Implement countermeasures
  - Verify countermeasures are effective
    - Upgrade or reconfigure
  - Document – Plan of Actions and Milestones (POAMS)

Overlapping Countermeasures

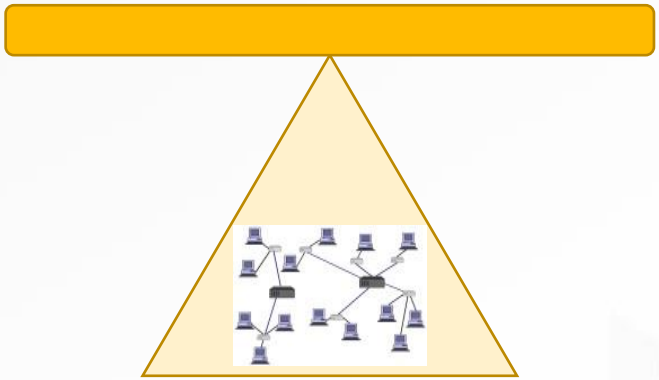
TOWSON UNIVERSITY

- Vulnerability = weakness
  - Does NOT present a risk
- Threat does not present a risk
- Risk = threat exploits a vulnerability (must be combined)
- Mitigate risks through countermeasures
  - Overlapping
    - Defense in depth
    - Minimize false positives

What is the right balance?

TOWSON UNIVERSITY

Cost of Risk Cost to fix



Step #5 Risk Control

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce impact (mitigation)
  - Understand consequences and accept risk (acceptance)

Risk Response Options

TOWSON UNIVERSITY

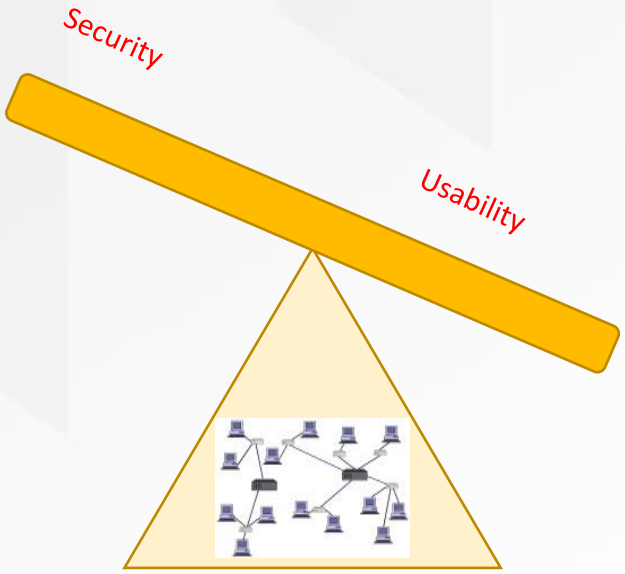
Now What?

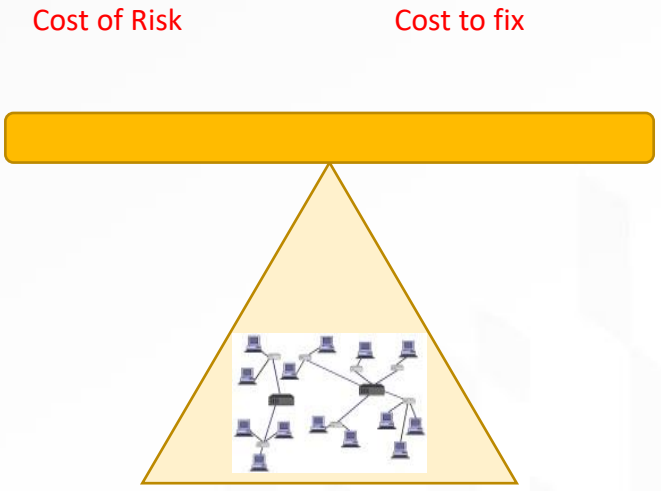
Techniques:

- Avoidance
  - Eliminate the source of the risk
  - Eliminate the expose of assets to the risk
- Share or Transfer (insurance)
- Mitigation – reduce the vulnerability (likelihood or impact)
- Accept the risk- take no action

Risk Response

- The action taken to manage or treat the risks
- Not all risks are created equal or should be treated the same
- Goal – identify the risks, determine the <u>appropriate</u> actions





Avoidance

- Attempts to prevent exploitation of the vulnerability
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods of risk avoidance:
  - Application of policy
  - Training and education
  - Applying technology

Transference

TOWSON UNIVERSITY

- Control approach that attempts to shift risk to other assets, processes, or organizations
- If lacking, organization should hire individuals/firms that provide security management and administration expertise
- Organization may then transfer risk associated with management of complex systems to another organization experienced in dealing with those risks

Mitigation

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans:
  - Incident response plan (IRP)
  - Disaster recovery plan (DRP)
  - Business continuity plan (BCP)

Acceptance

TOWSON UNIVERSITY

- Doing nothing to protect a vulnerability and accepting the outcome of its exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection
- Risk appetite describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls

Selecting a Risk Control Strategy

TOWSON UNIVERSITY

- Level of threat and value of asset play major role in selection of strategy
- Rules of thumb on strategy selection can be applied:
  - When a vulnerability exists
  - When a vulnerability can be exploited
  - When attacker's cost is less than potential gain
  - When potential loss is substantial

Cost Benefit Analysis (CBA)

TOWSON UNIVERSITY

- Most common approach for information security controls is economic feasibility of implementation
- CBA is begun by evaluating worth of assets to be protected and the loss in value if those assets are compromised
- The formal process to document this is called cost benefit analysis or economic feasibility study

Cost Benefit Analysis (CBA)

- Items that impact cost of a control or safeguard include: cost of development; training fees; implementation cost; service costs; cost of maintenance
- Benefit is the value an organization realizes by using controls to prevent losses associated with a vulnerability
- Asset valuation is process of assigning financial value or worth to each information asset; there are many components to asset valuation

Legal Compliance Impacts

- HIPAA = Health Insurance Portability & Accountability Act
- SOX = Sarbanes-Oxley Act
- FISMA = Federal Information Security Modernization Act
- FERPA = Family Education Rights & Privacy Act
- CIPA = Children's Internet Protection Act
- PCI DSS = Payment Card Industry Data Security Standards

For NOT in Compliance (Penalties)

Summary

TOWSON UNIVERSITY

- Risk identification
  - A risk management strategy enables identification, classification, and prioritization of organization's information assets
  - Residual risk: risk remaining to the information asset even after the existing control is applied
- Risk control: process of taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of components of an information system

Summary - Minimizing Risk
Risk-Based Approach to Security

TOWSON UNIVERSITY

- Assess the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.
- Determine the levels of information security appropriate to protect information and information systems.
- Implement policies and procedures to cost-effectively reduce risks to an acceptable level.
- Regularly test and evaluate information security controls and techniques to ensure effective implementation and improvement of such controls and techniques.

Summary

- Risk Management is a recognition that you cannot protect your company from everything.
- It is about prioritization and the acceptance of risk.
- IT should NOT decide how much residual risk is acceptable.