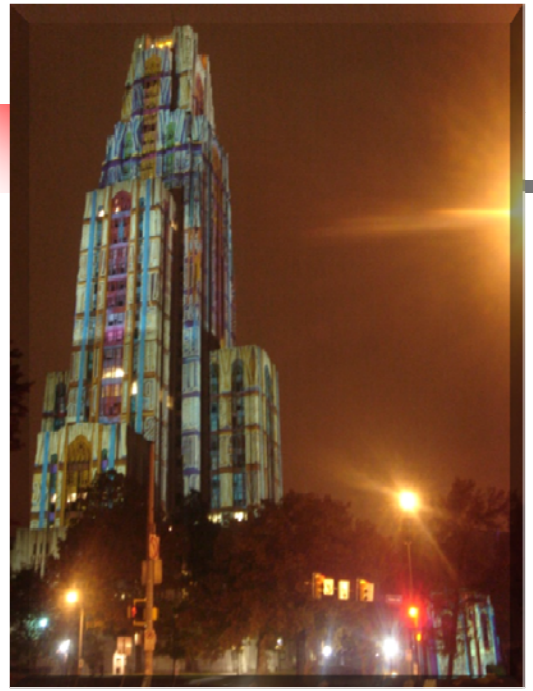
IS 2150 / TEL 2810
Information Security & Privacy



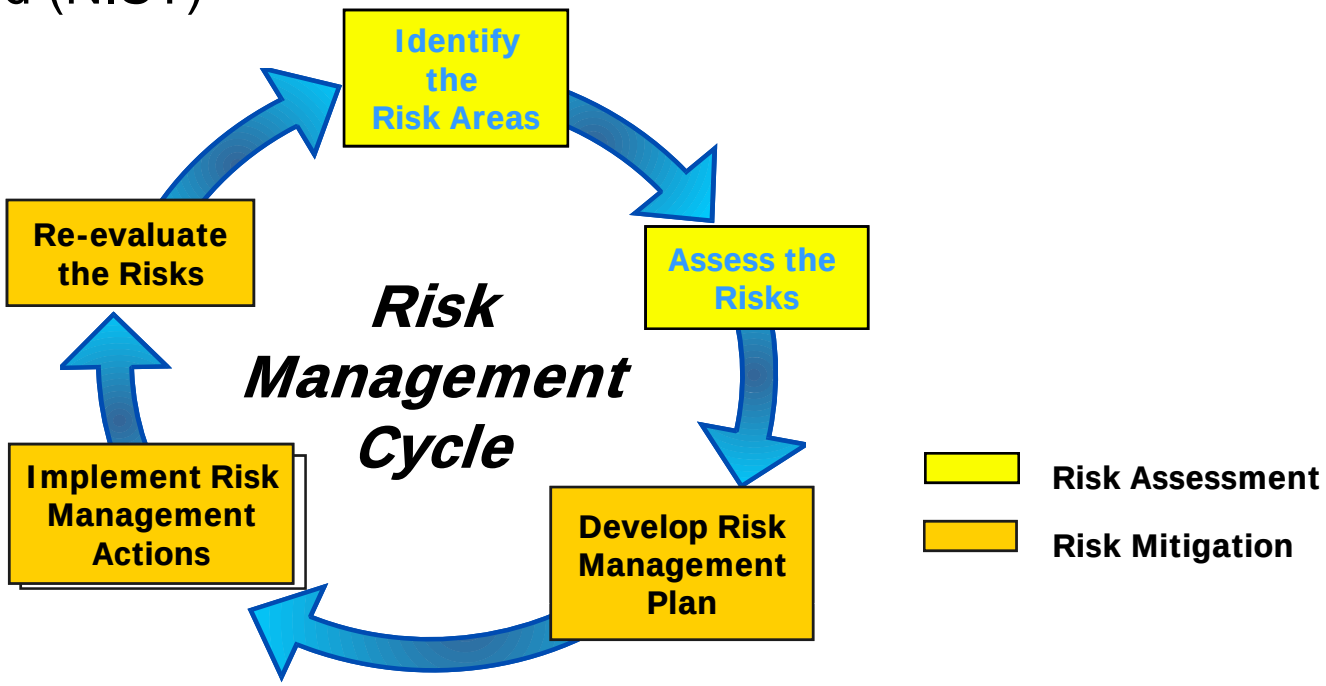
James Joshi
Professor, SIS

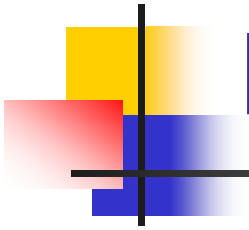
Nov 1, 2016

Risk Management

Risk Management

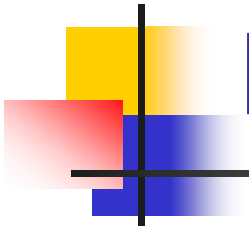
- The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected (NIST)





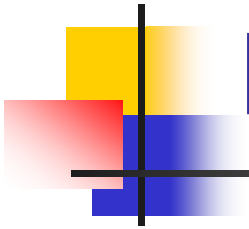
Risk

- The *likelihood* that a particular *threat* using a specific *attack*, will exploit a particular *vulnerability* of a system that results in an undesirable *consequence* (NIST)
  - *Likelihood* of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event



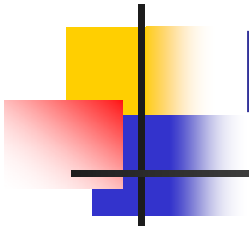
Risk Assessment/Analysis

- A process of analyzing *threats* to and *vulnerabilities* of an information system and the *potential impact* the loss of information or capabilities of a system would have
  - List the threats and vulnerabilities
  - List possible control and their cost
  - Do cost-benefit analysis
    - Is cost of control more than the expected cost of loss?
- The resulting analysis is used as a basis for identifying appropriate and cost-effective counter-measures
  - Leads to proper security plan



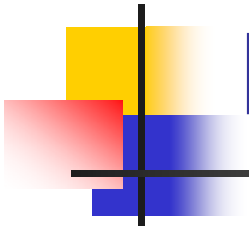
Risk Assessment steps

- Identify assets
  - Hardware, software, data, people, supplies
- Determine vulnerabilities
  - Intentional errors, malicious attacks, natural disasters
- Estimate likelihood of exploitation
  - Considerations include
    - Presence of threats
    - Tenacity/strength of threats
    - Effectiveness of safeguards
  - Delphi approach
    - Raters provide estimates that are distributed and re-estimated



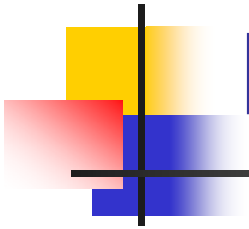
Risk Assessment steps (2)

- Compute expected annual loss
  - Physical assets can be estimated
  - Data protection for legal reasons
- Survey applicable (new) controls
  - If the risks of unauthorized access is too high, access control hardware, software and procedures need to be re-evaluated
- Project annual savings of control



Example 1

- Risks:
  - disclosure of company confidential information,
  - computation based on incorrect data
- Cost to correct data: $1,000,000
  - @10% liklihood per year: $100,000
  - Effectiveness of access control sw:60%: -$60,000
  - Cost of access control software: +$25,000
  - Expected annual costs due to loss and controls:
    - $100,000 - $60,000 + $25,000 = $65,000
  - Savings:
    - $100,000 - $65,000 = $35,000



Example 2

- Risk:
  - Access to unauthorized data and programs
    - 100,000 @ 2% likelihood per year: $2,000
  - Unauthorized use of computing facility
    - 100,000 @ 40% likelihood per year: $4,000
- Expected annual loss:

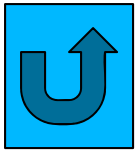
  $6,000
- Effectiveness of network control: 100%

  -$6,000

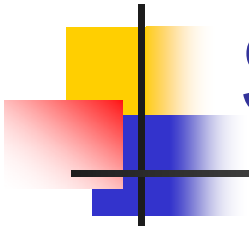
Example 2 (2)

- Control cost
  - Hardware +$10,000
  - Software +$4,000
  - Support personnel +$40,000
  - Annual cost: +$54,000
  - Expected annual cost
    - (6000-6000+54000) +$54,000
  - Savings
    - (6000 – 54,000) -$48,000

Some Arguments against Risk Analysis



- Not precise
  - Likelihood of occurrence
  - Cost per occurrence
- False sense of precision
  - Quantification of cost provides false sense of security
- Immutability
  - Filed and forgotten!
  - Needs annual updates
- No scientific foundation (not true)
  - Probability and statistics



Summary

- Vulnerability Analysis – taxonomy
- Risk Management – cost benefit analysis