Chapter 1: Measuring and Weighing Risk
Chapter 1: Measuring and Weighing Risk

• Explain the importance of risk related concepts
• Given a scenario, implement risk mitigation strategies
• Summarize risk management best practices
• Implementing Assessment Tools and Techniques to Discover Security Threats and Vulnerabilities
• Explaining the Importance of Data Security
Risk Assessment

• Risk Assessment (Risk Analysis)
  – Risk Assessment
    • Deals with the threats, vulnerabilities, and impacts of a loss of information-processing capabilities or information itself.

  – Key Components of Risk Assessment:
    • Risks to Which the Organization is Exposed
    • Risks That Need Addressing
    • Coordination with BIA
Computing Risk Assessment

• Methods of Measurement
  – Annualized Rate of Occurrence (ARO)
    • Likelihood, often from historical data, of an event occurring within a year.
  – ARO Can be Used in Conjunction With:
    • Single Loss Expectancy (SLE)
    • Annual Loss Expectancy (ALE)
    • Formula:
      \[ \text{SLE} \times \text{ARO} = \text{ALE} \]
Computing Risk Assessment Continued

• Risk Assessment Can be Qualitative or Quantitative
  – Qualitative
    • Opinion-base and subjective
  – Quantitative:
    • Cost-based and objective
Acting on Your Risk Assessment

• **Risk Avoidance**
  – Involves identifying a risk and making the decision to no longer engage in actions associated with that risk.

• **Risk Transference**
  – Sharing some of the burden of the risk with someone else.

• **Risk Mitigation**
  – Accomplished anytime steps are taken to reduce risk.
Acting on Your Risk Assessment

• Risk Deterrence
  – Involves understanding something about the enemy and letting them know harm can come their way if they cause harm to you.

• Risk Acceptance
  – Often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition.
Risks and Cloud Computing

• Cloud Computing:
  – Using the Internet to host services and data instead of hosting it locally

• Three Ways to Implement Cloud Computing:
  1. Platform as a Service
  2. Software as a Service
  3. Infrastructure as a Service
Risks and Cloud Computing

- Risk-related Issues Associated with Cloud Computing:
  - Regulatory Compliance
  - User privileges
  - Data Integration/Segregation
Risks Associated with Virtualization

• Breaking Out of the Virtual Machine
• Network and Security Controls Can Intermingle
  – Hypervisor: the virtual machine monitor-the software that allows the virtual machines to exist
Developing Policies, Standards, and Guidelines

• Implementing Policies
  – Policies provide people in an organization with guidance about their expected behavior.
  – Well-written policies are clear and concise, and outline the consequences when they are not followed.
Key Areas of a Good Policy

• Scope Statement
  – Outlines what the policy intends to accomplish and which documents, laws, and practices the policy addresses

• Policy Overview Statement
  – Provides goal of the policy, why it’s important, and how to comply with it

• Policy Statement
  – Should be as clear and unambiguous as possible

• Accountability Statement
  – Provides additional information to readers about who to contact if a problem is discovered

• Exception Statement
  – Provides specific guidance about the procedure or process that must be followed in order to deviate from the policy
Chapter 1: Measuring and Weighing Risk

Incorporating Standards: Five Points

1. Scope and Purpose
2. Roles and Responsibilities
3. Reference Documents
4. Performance Criteria
5. Maintenance and Administrative Requirements
Following Guidelines

• Guidelines
  – Help an organization implement or maintain standards by providing information on how to accomplish policies and maintain standards

Four Minimum Contents of Good Guidelines
1. Scope and Purpose
2. Roles and Responsibilities
3. Guideline Statements
4. Operational Considerations
Business Policies Primary Areas of Concern

• Separation of duties
• Due care
• Physical access control
• Document disposal and destruction
• Privacy policy
• Acceptable use
• Security policy
• Mandatory vacations
• Job rotation
• Least privilege
Chapter 1: Measuring and Weighing Risk

• False Positives
  – Events that aren’t really incidents

• Change Management
  – Structured approach that is followed to secure the company’s assets

• Incident Management
  – Steps followed when events occur
Redundant Array of Independent Disks

• *Redundant Array of Independent Disks (RAID)*
  – is a technology that uses multiple disks to provide fault tolerance

Several designations for RAID levels:

• RAID Level 0 RAID 0 is *disk striping.*
• RAID Level 1 RAID 1 is *disk mirroring.*
• RAID Level 3 RAID 3 is *disk striping with a parity disk.*
• RAID Level 5 RAID 5 is *disk striping with parity*
Tabletop Exercise

• Involves individuals sitting around a table with a facilitator discussing situations that could arise and how best to respond to them.

• Advantage is that there is very little cost to it (the time of the participants), and it allows key personnel to mentally walk through emergencies in a low-stress format.

• Disadvantage is its lack of realism.