TEL2813/IS2820
Security Management

Risk Management:
Assessing and Controlling Risk
Lecture 8
Feb 17, 2005

Introduction

- Competitive Disavantage
  - To keep up with the competition, organizations must design and create a safe environment in which business processes and procedures can function
- This environment must
  - Maintain confidentiality and privacy
  - Assure the integrity and availability of organizational data

Use principles of risk management

Risk Control Strategies

- Choose basic control risks strategy :
  - **Avoidance:**
    - applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
  - **Transference:**
    - shifting the risk to other areas or to outside entities
  - **Mitigation:**
    - reducing the impact should the vulnerability be exploited
  - **Acceptance:**
    - understanding the consequences and accept the risk without control or mitigation

Avoidance

- Attempts to prevent the exploitation of the vulnerability
- Accomplished through:
  - Application of policy
  - Application of training and education
  - Countering threats
  - Implementation of technical security controls and safeguards

Transference

- Attempts to shift the risk to other assets, other processes, or other organizations
- May be accomplished by
  - Rethinking how services are offered
  - Revising deployment models
  - Outsourcing to other organizations
  - Purchasing insurance
  - Implementing service contracts with providers

Mitigation

- Attempts to reduce the damage caused by the exploitation of vulnerability
  - by means of planning and preparation,
- Includes three types of plans:
  - Disaster recovery plan (DRP)
  - Incident response plan (IRP)
  - Business continuity plan (BCP)
- Depends upon
  - the ability to detect and respond to an attack as quickly as possible

Summaries of Mitigation Plans

TABLE 8-1 Summaries of Mitigation Plans

Plan	Description	Example	When deployed	Timeframe
Incident Response Plan (IRP)	Actions an organization takes during incidents (attacks)	■ List of steps to be taken during disaster ■ Intelligence gathering ■ Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery Plan (DRP)	■ Preparations for recovery should a disaster occur ■ Strategies to limit losses before and during disaster ■ Step-by-step instructions to regain normalcy	■ Procedures for the recovery of lost data ■ Procedures for the reestablishment of lost services ■ Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity Plan (BCP)	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	■ Preparation steps for activation of secondary data centers ■ Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term operation

Acceptance

- Acceptance is the choice to do nothing to protect an information asset and to accept the loss when it occurs
- This control, or lack of control, assumes that it may be a prudent business decision to
  - Examine alternatives
  - Conclude the cost of protecting an asset does not justify the security expenditure

Acceptance (Continued)

- Only valid use of acceptance strategy occurs when organization has:
  - Determined level of risk to information asset
  - Assessed probability of attack and likelihood of a successful exploitation of vulnerability
  - Approximated ARO of the exploit
  - Estimated potential loss from attacks
  - Performed a thorough cost benefit analysis
  - Evaluated controls using each appropriate type of feasibility
  - Decided that the particular asset did not justify the cost of protection

Risk Control Strategy Selection

- Risk control involves
  - selecting one of the four risk control strategies for the vulnerabilities present within the organization
- Acceptance of risk
  - If the loss is within the range of losses the organization can absorb, or
  - if the attacker's gain is less than expected costs of the attack,
- Otherwise, one of the other control strategies will have to be selected

Risk Handling Action Points

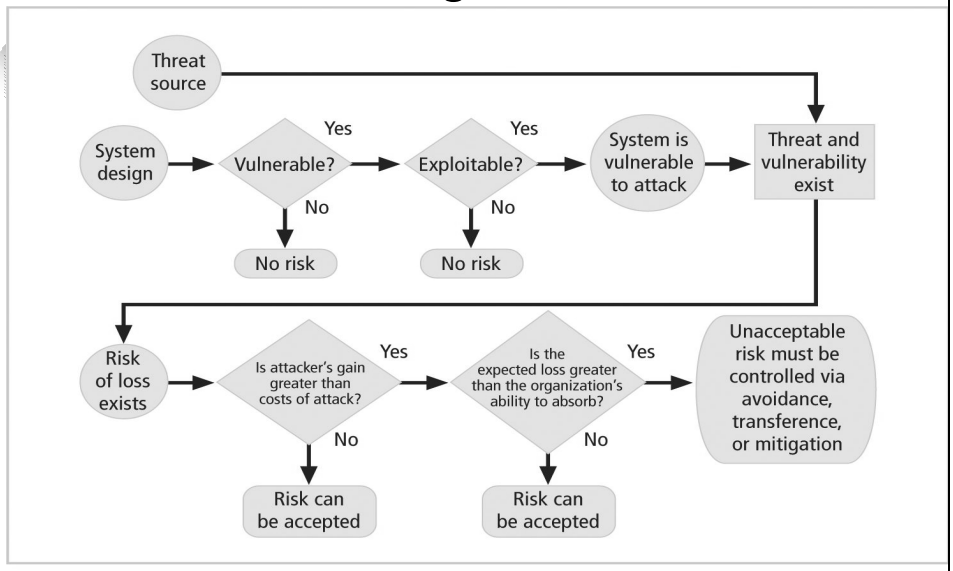


FIGURE 8-2 Risk-Handling Action Points

Risk Control Strategy Selection Some rules

- When a vulnerability exists:
  - Implement security controls to reduce the likelihood of a vulnerability being exercised
- When a vulnerability can be exploited:
  - Apply layered controls to minimize the risk or prevent occurrence
- When the attacker's potential gain is greater than the costs of attack:
  - Apply protections to increase the attacker's cost, or reduce the attacker's gain, using technical or managerial controls
- When potential loss is substantial:
  - Apply design controls to limit the extent of the attack, thereby reducing the potential for loss

Evaluation, Assessment, And Maintenance Of Risk Controls

- Once a control strategy has been selected and implemented
  - Effectiveness of controls should be monitored and measured on an ongoing basis to determine its effectiveness
  - Accuracy of estimated risk that will remain after all planned controls are in place

The Risk Control Cycle

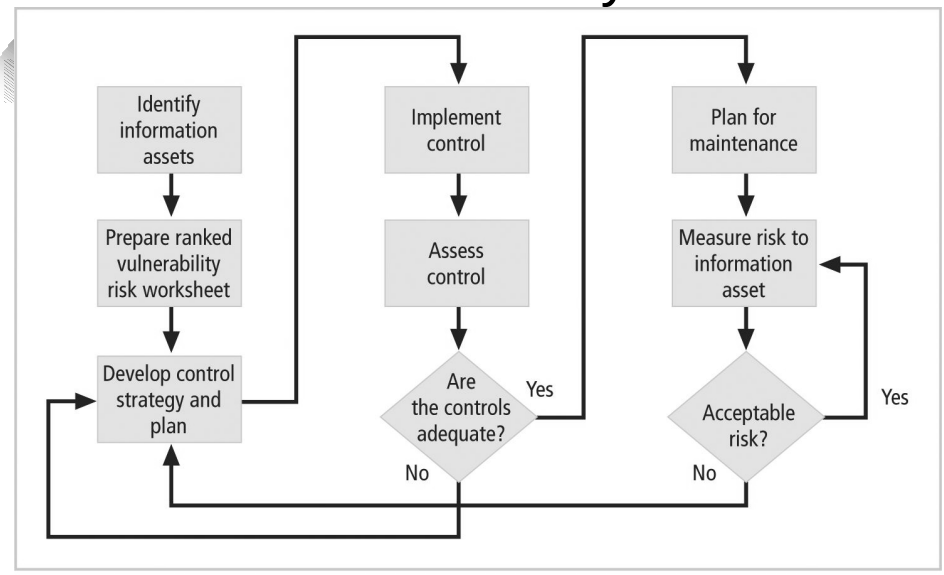


FIGURE 8-3 Risk Control Cycle

Categories of Controls

- Implementing controls or safeguards
  - To control risk by means of
    - avoidance,
    - mitigation,
    - transference
- Controls can be one of four categories:
  - Control function
  - Architectural layer
  - Strategy layer
  - Information security principle

Control Function

- Preventive controls
  - Stop attempts to exploit a vulnerability by implementing enforcement of an organizational policy or a security principle
  - Use a technical procedure, or some combination of technical means and enforcement methods
- Detective controls
  - Alerts about violations of security principles, organizational policies, or attempts to exploit vulnerabilities
  - Use techniques such as audit trails, intrusion detection, and configuration monitoring

Architectural Layer

- Some controls apply to one or more layers of an organization's technical architecture
- Possible architectural layers include the following:
  - Organizational policy
  - External networks & Extranets
  - Demilitarized zones
  - Intranets
  - Network devices that interface network zones
  - Systems
  - Applications

Strategy Layer

- Controls are sometimes classified by the risk control strategy they operate within:
  - Avoidance
  - Mitigation
  - Transference
- Note that the acceptance strategy is not an option since it involves the absence of controls

Information Security Principle

- Risk controls operate within one or more of the commonly accepted information security principles:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Authorization
  - Accountability
  - Privacy

Feasibility Studies and Cost Benefit Analysis

- Information about the consequences of the vulnerability must be explored
  - Before deciding on the strategy for a specific vulnerability,
- Determine advantage or disadvantage of a specific control
  - Primary means are based on the value of information assets that control is designed to protect

Cost Benefit Analysis (CBA)

- Economic Feasibility
  - criterion most commonly used when evaluating a project that implements information security controls and safeguards
- Should begin a CBA by evaluating
  - Worth of the information assets to be protected
  - Loss in value if those information assets are compromised

Cost Benefit Analysis or *Economic Feasibility Study*

Cost

- It is difficult
  - to determine the value of information,
  - to determine the cost of safeguarding it
- Some of the items that affect the cost of a control or safeguard include:
  - Cost of development or acquisition of hardware, software, and services
  - Training fees
  - Cost of implementation
  - Service costs
  - Cost of maintenance

Benefit

- Benefit is
  - the value to the organization of using controls to prevent losses associated with a specific vulnerability
- Usually determined by
  - Valuing the information asset or assets exposed by vulnerability
  - Determining how much of that value is at risk and how much risk there is for the asset
- This is expressed as
  - Annualized Loss Expectancy (ALE)

Asset Valuation

- Asset valuation is
  - a challenging the process of assigning financial value or worth to each information asset
- Value of information differs
  - Within organizations and between organizations
  - Based on information characteristics and perceived value of that information
- Valuation of assets involves:
  - Estimation of real and perceived costs associated with design,
  - development, installation, maintenance, protection, recovery, and defense against loss and litigation

Asset Valuation Components

- Some of the components of asset valuation include:
  - Value retained from the cost of creating the information asset
  - Value retained from past maintenance of the information asset
  - Value implied by the cost of replacing the information
  - Value from providing the information
  - Value acquired from the cost of protecting the information
  - Value to owners
  - Value of intellectual property
  - Value to adversaries
  - Loss of productivity while the information assets are unavailable
  - Loss of revenue while information assets are unavailable

Asset Valuation Approaches

- Organization must be able to place a dollar value on each information assets it owns, based on:
  - How much did it cost to create or acquire?
  - How much would it cost to recreate or recover?
  - How much does it cost to maintain?
  - How much is it worth to the organization?
  - How much is it worth to the competition?

Asset Valuation Approaches (Continued)

- Potential loss is that which could occur from the exploitation of vulnerability or a threat occurrence
- The questions that must be asked include:
  - What loss could occur, and what financial impact would it have?
  - What would it cost to recover from the attack, in addition to the financial impact of damage?
  - What is the single loss expectancy for each risk?

Asset Valuation Techniques

- Single loss expectancy (SLE):
  - calculation of value associated with most likely loss from an attack
  - Based on estimated asset value and expected percentage of loss that would occur from attack:
    SLE = asset value (AV) x exposure factor (EF)
    - *EF = the percentage loss that would occur from a given vulnerability being exploited*
- In most cases,
  - probability of a threat occurring is the probability of an attack within a given time frame
  - Commonly referred to as the ARO, or annualized rate of occurrence

The Cost Benefit Analysis (CBA) Formula

- CBA determines whether or not a control alternative is worth its associated cost
- CBAs may be calculated
  - Before a control or safeguard is implemented to determine if the control is worth implementing
    OR
  - After controls have been implemented and have been functioning for a time:

    CBA = ALE(prior) – ALE(post) – ACS

The Cost Benefit Analysis (CBA) Formula

- ALE(prior to control) is
  - the annualized loss expectancy of the risk before the implementation of the control
- ALE(post control) is
  - the ALE examined after the control has been in place for a period of time
- ACS is
  - the annual cost of the safeguard

Other Feasibility Approaches

- Organizational feasibility analysis
  - examines how well the proposed information security alternatives will contribute to operation of an organization
- Operational feasibility analysis

  Addresses user acceptance and support, management acceptance and support, and overall requirements of organization's stakeholders

Other Feasibility Approaches

- Technical feasibility analysis
  - examines whether or not the organization has or can acquire the technology to implement and support the alternatives
- Political feasibility analysis
  - defines what can and cannot occur based on the consensus and relationships between the communities of interest

Benchmarking

- Benchmarking:
  - Seeking out and studying practices of other organizations that produce desired results
  - Measuring differences between how organizations conduct business
- When benchmarking, an organization typically uses one of two measures to compare practices:
  - Metrics-based measures
    - comparisons based on numerical standards
  - Process-based measures
    - generally less focused on numbers and are more strategic

Benchmarking (Continued)

- In the field of information security, two categories of benchmarks are used:
  - Standards of due care and due diligence, and
  - Best practices
- Within best practices, the gold standard is a subcategory of practices that are typically viewed as “the best of the best”

Due Care and Due Diligence

- For legal reasons, an organization may be forced to adopt a certain minimum level of security
- Due Care
  - adopt levels of security for legal defense,
  - need to show that they have done what any prudent organization would do in similar circumstances
- Due diligence
  - demonstration that organization is persistent in ensuring implemented standards continue to provide required level of protection

Best Business Practices

- Best business practices:
  - security efforts that seek to provide a superior level of performance
  - Are among the best in the industry,
  - balancing access to information with adequate protection, while maintaining a solid degree of fiscal responsibility
- Companies with best practices may not be the best in every area

The Gold Standard

- Even the best business practices are not sufficient for some organizations
- These organizations aspire to set the standard by implementing the most protective, supportive, and yet fiscally responsible standards they can
- The gold standard
  - is a defining level of performance that demonstrates a company's industrial leadership, quality, and concern for the protection of information

Applying Best Practices

- Address the following questions:
  - Does your organization resemble the organization that is implementing the best practice under consideration?
  - Is your organization in a similar industry?
  - Does your organization face similar challenges?
  - Is your organizational structure similar to the organization from which you are modeling the best practices?
  - Can your organization expend resources that are in line with the requirements of the best practice?
  - Is your organization in a similar threat environment as the one cited in the best practice?

Problems with Benchmarking and Best Practices

- Organizations don't talk to each other
- No two organizations are identical
- Best practices are a moving target
- Simply knowing what was going on a few years ago does not necessarily indicate what to do next

Baselining

- Baselining is the analysis of measures against established standards
- In information security, baselining is the comparison of security activities and events against the organization's future performance
- The information gathered for an organization's first risk assessment becomes the baseline for future comparisons

Risk Appetite

- Risk appetite
  - defines the quantity and nature of risk that organizations are willing to accept, as they evaluate the trade-offs between perfect security and unlimited accessibility
- Reasoned approach to risk is one that
  - balances expense against possible losses if exploited

Residual Risk

- When vulnerabilities have been controlled as much as possible, there is often remaining risk that has not been completely accounted for — residual risk
- Residual Risk:
  - Risk from a threat less the effect of threat-reducing safeguards plus
  - Risk from a vulnerability less the effect of vulnerability-reducing safeguards plus
  - Risk to an asset less the effect of asset value-reducing safeguards

Residual Risk

- The significance of residual risk
  - must be judged within the context of an organization's risk appetite
- The goal of information security
  - is not to bring residual risk to zero,
  - but to bring it in line with an organization's risk appetite

Documenting Results

- When risk management program has been completed, series of proposed controls are prepared
  - Each justified by one or more feasibility or rationalization approaches
- At minimum, each information asset-threat pair should have a documented control strategy that
  - Clearly identifies any residual risk remaining after the proposed strategy has been executed

Documenting Results

- Some organizations document outcome of control strategy for each information asset-threat pair in an action plan
- Includes:
  - Concrete tasks, each with accountability assigned to an organizational unit or to an individual

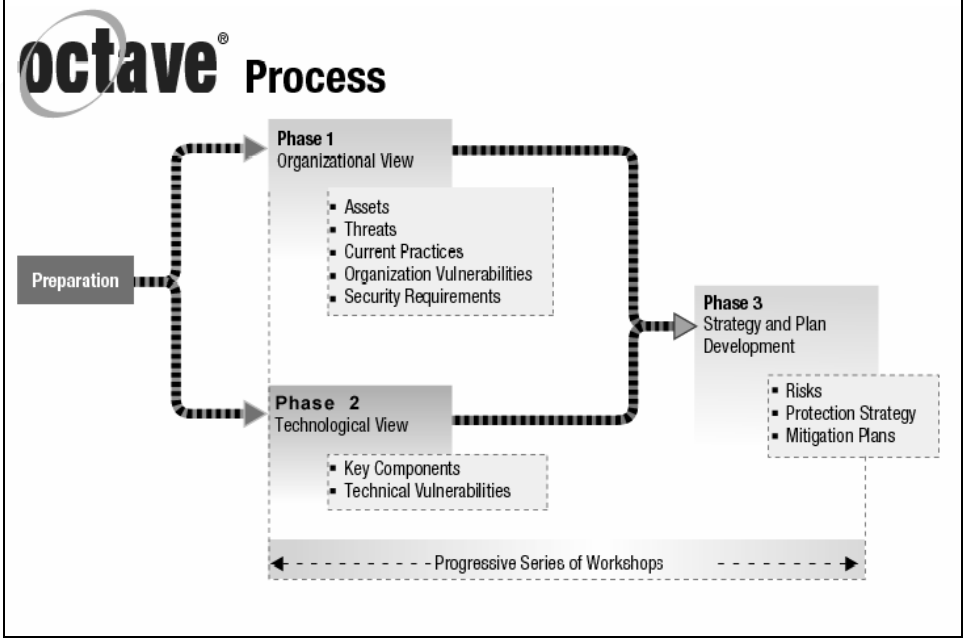
Qualitative Measures

- Quantitative assessment performs asset valuation with actual values or estimates
- An organization could determine that it cannot put specific numbers on these values
- Organizations could use qualitative assessments instead, using scales instead of specific estimates

Delphi Approach

The OCTAVE Method

- Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠) Method:
  - Defines essential components of a comprehensive, systematic, context-driven, self-directed information security risk evaluation
- By following OCTAVE Method, organization can
  - make information protection decisions based



Phases of The OCTAVE Method

- Phase 1: Build Asset-Based Threat Profiles
  - Organizational evaluation
  - Key areas of expertise within organization are examined to elicit important knowledge about:
    - Information assets
    - Threats to those assets
    - Security requirements of assets
    - What organization is currently doing to protect its information assets
  - Weaknesses in organizational policies and practice

Phases of The OCTAVE Method (Continued)

- Phase 2: Identify Infrastructure Vulnerabilities
  - Evaluation of information infrastructure
  - Key operational components of information technology infrastructure are examined for weaknesses (technology vulnerabilities) that can lead to unauthorized action

Phases of The OCTAVE Method (Continued)

- Phase 3: Develop Security Strategy and Plans
  - Risks are analyzed in this phase
  - Information generated by organizational and information infrastructure evaluations (Phases 1 and 2) is analyzed to:
    - Identify risks to organization
    - Evaluate risks based on their impact to the organization's mission
  - Organization protection strategy and risk mitigation plans for the highest priority risks are developed

Important Aspects of the OCTAVE Method

- The OCTAVE Method:
  - Self directed
  - Requires analysis team to conduct evaluation and analyze information
- Basic tasks of the team are to:
  - Facilitate knowledge elicitation workshops of Phase 1
  - Gather any necessary supporting data
  - Analyze threat and risk information
  - Develop a protection strategy for the organization
  - Develop mitigation plans to address risks to the organization's critical assets

Important Aspects of the OCTAVE Method (Continued)

- OCTAVE Method:
  - Uses workshop-based approach for gathering information and making decisions
  - Relies upon the following major catalogs of information:
    - Catalog of practices: collection of good strategic and operational security practices
    - Threat profile: range of major sources of threats that an organization needs to consider
    - Catalog of vulnerabilities: collection of vulnerabilities based on platform and application

Phases & Processes of the OCTAVE Method

- Each phase of the OCTAVE Method contains two or more processes. Each process is made of activities.
- Phase 1: Build Asset-Based Threat Profiles
  - Process 1: Identify Senior Management Knowledge
  - Process 2: Identify Operational Area Management Knowledge
  - Process 3: Identify Staff Knowledge
  - Process 4: Create Threat Profiles

Phases & Processes of the OCTAVE Method (Continued)

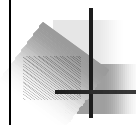
- Phase 2: Identify Infrastructure Vulnerabilities
  - Process 5: Identify Key Components
  - Process 6: Evaluate Selected Components
- Phase 3: Develop Security Strategy and Plans
  - Process 7: Conduct Risk Analysis
  - Process 8: Develop Protection Strategy

Preparing for the OCTAVE Method

- Obtain senior management sponsorship of OCTAVE
- Select analysis team members.
- Train analysis team
- Select operational areas to participate in OCTAVE
- Select participants
- Coordinate logistics
- Brief all participants

The OCTAVE Method

- For more information, you can download the Octave[SM] method implementation guide from www.cert.org/octave/omig.html



Summary

- Introduction
- Risk Control Strategies
- Risk Control Strategy Selection
- Categories of Controls
- Feasibility Studies and Cost-Benefit Analysis
- Risk Management Discussion Points
- Recommended Risk Control Practices
- The OCTAVE Method