

Effective Risk Analysis

Thomas R. Peltier, CISSP



Driving eBusiness PerformanceSM

Effective Risk Analysis

- The dictionary defines RISK as "someone or something that creates or suggests a hazard". It is one of the many costs of doing business or providing a service today.
- Information security professionals know and understand that nothing ever runs smoothly for very long. Any manner of internal or external hazard or risk can cause a well running organization to lose competitive advantage, miss a deadline, or suffer embarrassment. As security professionals, management looks to us to provide a method that allows for the systematic review of risk, threats, hazards and concerns and provide cost-effective measures to lower risk to an acceptable level. This session will review the current practical application of cost-effective risk analysis.

- Frequently Asked Questions
 - Why should a risk analysis be conducted?
 - When should a risk analysis be conducted?
 - Who should conduct the risk analysis?
 - How long should a risk analysis take?
 - What can a risk analysis analyze?
 - What can the results of a risk analysis tell an organization?
 - Who should review the results of a risk analysis?
 - How is the success of the risk analysis measured?

- Risk Analysis as part of an organization-wide information quality assurance program
 - Supporting Business Objectives or Mission requires
 - Identification of customer requirements
 - Sensitivity of information
 - Availability of the system or application
 - Basic enterprise requirements include
 - Information classification
 - Business Impact Analysis (BIA)
 - Risk analysis
 - Intellectual property safeguards

- The goal of an enterprise-wide information quality assurance program is to preserve the:
 - Integrity
 - Confidentiality
 - Availability

- Information protection in quality assurance works with three key elements:
 - Integrity - the information is as intended without inappropriate modification or corruption
 - Confidentiality - the information is protected from unauthorized or accidental disclosure
 - Availability - authorized users can access applications and systems when required to do their job

- No matter what risk analysis process is used, the method is always the same:
 - Identify the asset
 - Ascertain the risk
 - Determine the vulnerability
 - Implement the corrective action
- Remember - sometimes accepting the risk is the appropriate corrective action.

- The risk analysis process
 - When identifying safeguards, it will be necessary to determine those already in place
 - 80% - 90% of the controls that mitigate risks are already in place
 - Safeguards will only lower risks to an acceptable level
 - 100% security is not the goal

- Definitions
 - Threat - an undesirable event
 - Vulnerability - a condition of a missing or ineffectively administered safeguard or control that allows a threat to occur with a greater impact or frequency or both.
 - Losses - these include direct and indirect loss
 - disclosure
 - integrity
 - denial of service

- Definitions
 - Safeguard/Control - a countermeasure that acts to prevent, detect, or minimize the consequences of threat occurrence.
 - Exposure Factor - how much impact or loss of asset value is incurred
 - from 0% to 100%
 - Single-time Loss Algorithm (SLA) - when a threat occurs, how much the loss of asset value is expected to be in monetary terms
 - Annualized Rate of Occurrence (ARO) - how often a threat might be expected to happen in one year.

- Method
- Annualized Loss Exposure (ALE) - a value presented by the classic risk analysis process indicating loss expectancy for a given threat;
- Consider the asset value (V), the likelihood vulnerability exposure factor (L) will equal the ALE.
 - $V \times L = ALE$

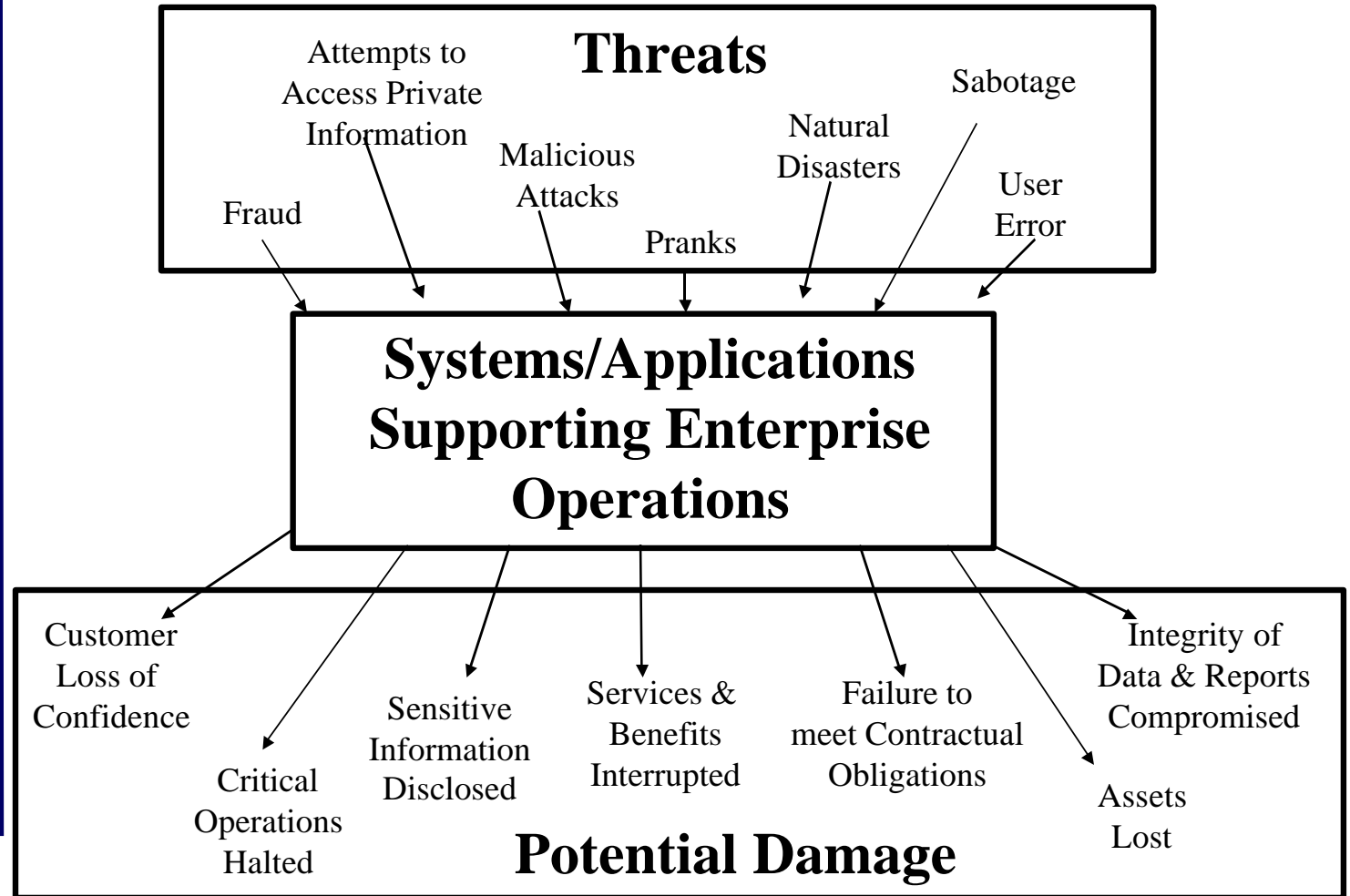
- Now that we've identified the Assets and the Threats, we are now going to spend some time trying to establish a bottom line value for the assets.
- One of the basic methods for determining expected loss is to multiply the Value of the asset (V) by the Likelihood of occurrence (L).
- This formula will produce an *Annual Loss Expectancy (ALE)*.

Annualized Loss Multiplier Table

Never		0.0
Once in 300 Years	1/300	0.00333
Once in 200 Years	1/200	0.005
Once in 100 Years	1/100	0.01
Once in 50 Years	1/50	0.02
Once in 25 Years	1/25	0.04
Once in 5 Years	1/5	0.20
Once in 2 Years	1/2	0.50
Yearly	1/1	1.0
Twice a Year	1/.5	2.0
Once a Month	12/1	12.0
Once a Week	52/1	52.0
Once a Day	365/1	365.0

- Exercise
- Now that we have identified the Value of our assets and the Likelihood of loss, let us use this information to do some quantitative risk analysis.
 - You have a \$3 million data center located in a flood area. A major flood that would destroy the data center occurs once every 100 years.
 - Compute the *ALE*.
 - Using the computed *ALE*, what is the probability that management would be willing to spend \$35,000 annually to control this threat?
 - Is it cost-effective?
-

- Risk Analysis Objectives
 - Identify potential undesirable or unauthorized events, “RISKS,” that could have a negative impact on the *Integrity, Confidentiality, or Availability* of information by, or flowing through, an application or system.
 - Identify potential “CONTROLS” to reduce or eliminate the impact of RISK events determined to be of MAJOR concern.



Information Security Objectives

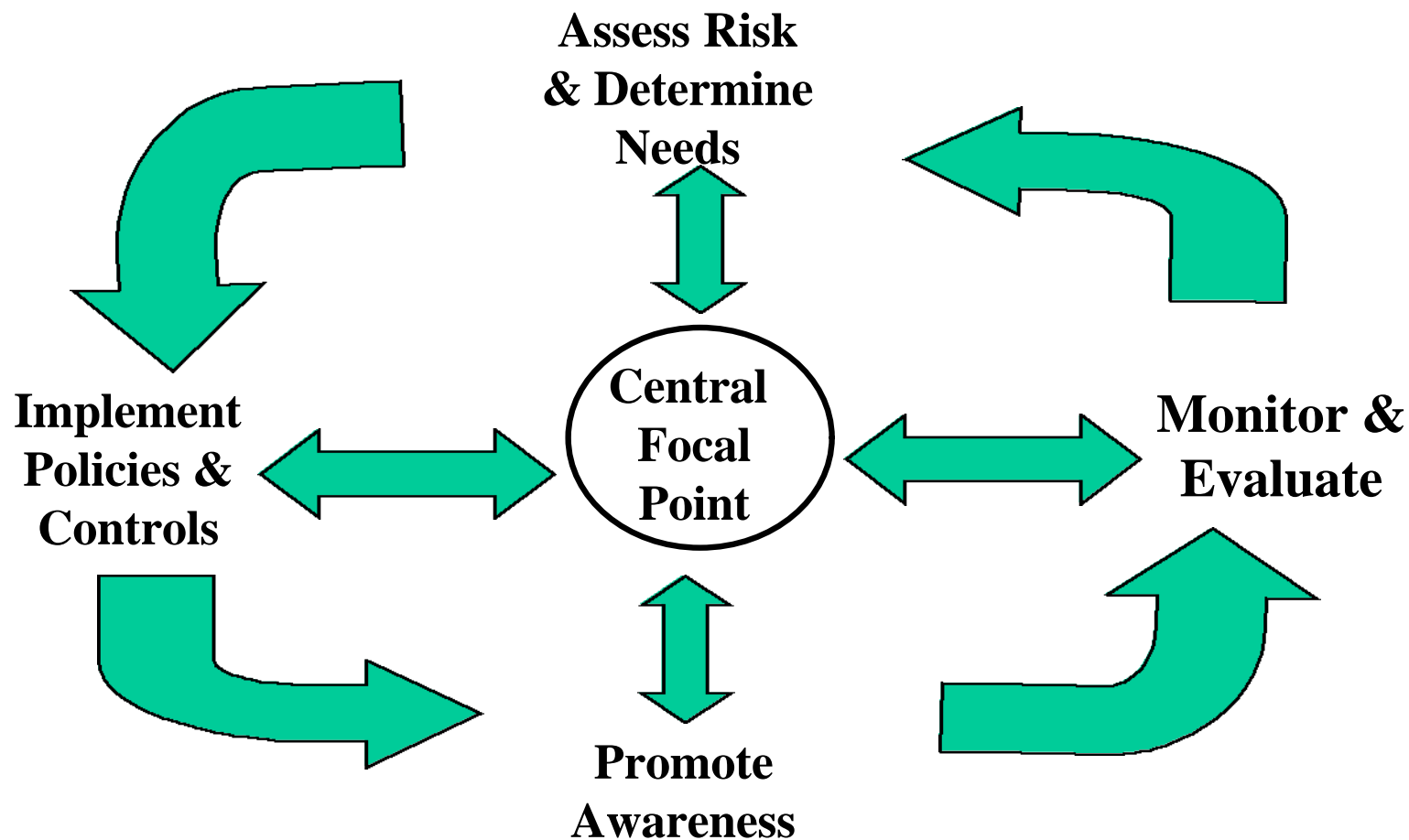
- Maintain customer, constituent, stockholder, or taxpayer confidence in the organization
- Protect confidentiality of sensitive information (personal, financial, trade secret, etc.)
- Protect sensitive operational data from inappropriate disclosure
- Avoid third-party liability for illegal or malicious acts committed with the organization's systems
- Ensure that organization computer, network, and data are not misused or wasted
- Avoid fraud
- Avoid expensive and disruptive incidents
- Comply with pertinent laws and regulations
- Avoid a hostile workplace atmosphere

Source GAO/AIMD 98-68

- Risk Management Principles
 - Assess risk and determine needs
 - Establish a central management focal point
 - Implement appropriate policies and related controls
 - Promote awareness
 - Monitor and evaluate policy and control effectiveness

Effective Risk Analysis

Risk Management Cycle



Sixteen Practices That Leading Use Organizations to Implement the Risk Management Cycle

Principle

- Assess Risk and Determine Needs

Practices

- Recognize information resources as essential organizational assets
- Develop practical risk assessment procedures that link security to business needs
- Hold program and business managers accountable
- Manage risk on a continuing basis

Sixteen Practices Used by Leading Organizations to Implement the Risk Management Cycle

Principle

- Establish a Central Management Focal Point

Practices

- Designate a central group to carry out key activities
- Provide the central group ready and independent access to senior executives
- Designate dedicated funding and staff
- Enhance staff professionalism and technical skills

Sixteen Practices Used by Leading Organizations to Implement the Risk Management Cycle

Principle

- Implement Appropriate Policies and Related Controls

Practices

- Link policies to business risks
- Distinguish between policies and guidelines
- Support policies through central security group

Sixteen Practices Used by Leading Organizations to Implement the Risk Management Cycle

Principle

- Promote Awareness

Practices

- Continually educate users and others on the risks and related policies
- Use attention-getting and user-friendly techniques

Sixteen Practices Used by Leading Organizations to Implement the Risk Management Cycle

Principle

- Monitor and Evaluate Policy and Control Effectiveness

Practices

- Monitor factors that affect risk and indicate security effectiveness
- Use results to direct future efforts and hold managers accountable
- Be alert to new monitoring tools and techniques

- Assess Risk and Determine Needs
 - Risk considerations and related cost-benefit trade-off are the primary focus of a security program.
 - Security is not an end in itself
 - Controls and safeguards are identified and implemented to address specific business risks
- Understanding the business risks associated with information security is the starting point of an effective risk analysis and management program

- “Information technology is an integral and critical ingredient for the successful functioning of major U.S. companies”
 - Deloitte & Touche LLP - Survey of American Business Leaders

- Organizations that are most satisfied with their risk analysis procedures are those that have defined a relatively simple process that can be adapted to various organizational units and involve a mix of individuals with knowledge of business operations and technical aspects of the enterprise's systems and security controls.*

*Source GAO/AIMD 98-68

- Different Methods - Qualitative vs. Quantitative

Quantitative Pros

- The results are based substantially on independently objective processes and metrics
- Great effort is put into asset value definition and risk mitigation
- Cost/benefit assessment effort is essential
- Results can be expressed in management-specific language
 - monetary value, percentages, probabilities

- Different Methods - Qualitative vs. Quantitative

Quantitative Cons

- Calculations are complex
- Historically only works well with a recognized automated tool and associated knowledge base
- Large amount of preliminary work
- Not presented on a personnel level
- Participants cannot be coached easily through the process
- Difficult to change directions
- Difficult to address ‘out-of-scope’ issues

- Different Methods - Qualitative vs. Quantitative

Qualitative Pros

- Calculations are simple
- Not necessary to determine \$ value of asset
- Not necessary to quantify threat frequency
- Easier to involve non-security and non-technical staff
- Provides flexibility in process and reporting

- Different Methods - Qualitative vs. Quantitative

Qualitative Cons

- Very subjective in nature
- Limited effort to develop monetary value for targeted assets
- No basis for the cost/benefit analysis of risk mitigation

Automated Checklists

- Typically ask business units a series of questions that prompt them to consider the impact of security controls
- The results are reported to senior management with:
 - stated business unit's compliance with security policy
 - planned actions to become compliant
 - willingness to accept risk
- Reports submitted to management and auditing

- Access Request Procedures
 - Connection to network requires Business Case which includes
 - risks associated with connection
 - Business case is reviewed by:
 - central security group
 - technical staff
 - requester

- Request for Deviation
 - In order to deviate from a “mandatory policy” the business unit submits letter explaining reason for deviation and recognizing the related risks.
 - Where necessary, alternative safeguards are identified
 - Request is reviewed by:
 - Business unit executive
 - Central security staff
 - Ultimate decision left with business unit

- **Facilitated Risk Analysis Process (FRAP)**
 - FRAP analyzes one system, application or segment of business process at a time
 - Team of individuals that include business managers and support groups is convened
 - Team brainstorms potential threats, vulnerabilities and resultant negative impacts to data integrity, confidentiality and availability
 - Impacts are analyzed to business operations
 - Threats and risks are prioritized

- Facilitated Risk Analysis Process (FRAP)
- The FRAP users believe that additional effort to develop precisely quantified risks are not cost effective because:
 - such estimates are time consuming
 - risk documentation becomes too voluminous for practical use
 - specific loss estimates are generally not needed to determine if controls are needed

- **Facilitated Risk Analysis Process (FRAP)**
 - After identifying and categorizing risks, the Team identifies controls that could mitigate the risk
 - A common group of 26 controls are used as a starting point
 - The decision for what controls are needed lies with the business manager
 - The Team's conclusions as to what risks exist and what controls are needed are documented along with a related action plan for control implementation

- Facilitated Risk Analysis Process (FRAP)
 - Each risk analysis session takes approximately 4 hours
 - Includes 7 to 15 people
 - Additional time is required to develop the action plan
 - Results remain on file for same time as Audit papers

- Facilitated Risk Analysis Process (FRAP)
 - Team does not attempt to obtain or develop specific numbers for threat likelihood or annual loss estimates
 - It is the team's experience that sets priorities
 - After identifying and categorizing risks, the groups identifies controls that can be implemented to reduce the risk

- The Risk and Control Summary Report is confidential and is owned by the Business manager requesting or sponsoring the FRAP

- Business managers bear the primary responsibility for determining the level of protection needed for information resources that support business operations.
- Security professionals must play a strong role in educating and advising management on exposures and possible controls.

- Government Accounting Office May 1998 Executive Guide for Information Security Management (GAO/AIMD 98-68)
 - “OMB’s 1996 revision of Circular A-130, Appendix III, recognizes that federal agencies have had difficulty in performing effective risk assessments . . . For this reason, the revised circular eliminates a long-standing federal requirement for formal risk assessments. Instead, it promotes a risk-based approach and suggests that, rather than trying to precisely measure risk, agencies should focus on generally assessing and managing risks.”

- We have discussed:
 - Why should a risk analysis be conducted?
 - When should a risk analysis be conducted?
 - Who should conduct the risk analysis?
 - How long should a risk analysis take?

- We have discussed:
 - What can a risk analysis analyze?
 - What can the results of a risk analysis tell an organization?
 - Who should review the results of a risk analysis?
 - How is the success of the risk analysis measured?

Comments?

Questions?

Critiques!

Effective Risk Analysis

Thomas R. Peltier, CISSP



Driving eBusiness PerformanceSM