



## Information Security ROI

Dr. Frank C. Braun  
Department of Business Informatics  
Northern Kentucky University

## IT as Expense

- IT departments have traditionally been viewed as cost centers
- The CIO / CTO has learned that a business case must be provided for IT initiatives
- Information Security initiatives must also figure out how to do the same thing..
- InfoSec Managers can't sell security initiatives based on fear alone.

## IT ROI

- ROI is about
  - Revenue Generation
  - Cost Savings
  - Increased Productivity
- IT must show for IT investments either some % increase in speed or flexibility, operational \$\$ savings, or new sales opportunities via IT...

## InfoSec ROI

- How can InfoSec
  - increase sales?
  - improve productivity?
  - Reduce Costs!
- How do you quantify InfoSec cost savings??
- How would you prepare a [Cost Benefit Analysis](#)?
- Can you calculate InfoSec ROI with Excel?

## InfoSec Risk Management

- Use a Risk-Based approach to *measure the value* of information security solutions.
- Risk-Based Benefit – The reduction in expected loss from security incidents
- Risk-Based Investment in Information Security *for future cost reduction...*

### Risk is

The likelihood of the occurrence of a vulnerability

*Multiplied by*

The value of the information asset

*Minus*

The percentage of risk mitigated by current controls

*Plus*

The uncertainty of current knowledge of the vulnerability

## Introduction

- To keep up with the competition, organizations must design and create a safe environment in which business processes and procedures can function with limited interruption
- This environment must maintain confidentiality and privacy and assure the integrity and availability of organizational data and information assets (i.e. SOX, HIPAA, & GLBA compliance)
- These objectives are met via the application of the principles of **risk management**

## Introduction

- **Risk management**: process of identifying and controlling risks facing an organization
- **Risk identification**: process of examining an organization's current information technology security situation
- **Risk control**: applying controls to reduce risks to an organization's data and information systems

## Accountability for Risk Management

- All communities of interest must work together in
  - Identifying risks
  - Assessing risks
  - Evaluating the risk controls
  - Determining which control options are cost-effective
  - Acquiring or installing the appropriate controls
  - Overseeing processes to ensure that the controls remain effective
  - Summarizing the findings

## Risk Identification

- Assets are targets of various threats and threat agents
- Risk management involves identifying organization's assets and identifying threats/vulnerabilities
- Risk identification begins with identifying organization's assets and assessing their value

10

## Create an Inventory of Information Assets

- Identify information assets, including people, procedures, data and information, software, hardware, and networking elements
- This step should be done without pre-judging the value of each asset; values will be assigned later in the process

## Example: Identify Hardware, Software, and Network Assets

- Whether automated or manual, the inventory process requires a certain amount of planning
- Determine which attributes of each of these information assets should be tracked
- That will depend on the needs of the organization and its risk management efforts

## Threat Identification

- Any organization typically faces a wide variety of threats
- If you assume that every threat can and will attack every information asset, then the project scope becomes too complex
- To make the process less unwieldy, each step in the threat identification and vulnerability identification process is managed separately and then coordinated at the end

## Identify and Prioritize Threats and Threat Agents

- Each threat presents a unique challenge to information security and must be handled with specific controls that directly address the particular threat and the threat agent's attack strategy
- Before threats can be assessed in the risk identification process, however, each threat must be further examined to determine its potential to affect the targeted information asset
- In general, this process is referred to as a threat assessment

## Some Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises in intellectual property	Patent, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information corruption	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Disruption of systems or infrastructure
Deliberate acts of theft	Illegal acquisition of equipment or information
Deliberate sabotage attacks	Viruses, worms, malware, denial-of-service
Problems in quality of service by service providers	Power and WAN quality of service issues from service providers
Process of failure	Fire, flood, earthquakes, lightning
Technical hardware failure or errors	Equipment failure
Technical software failure or errors	Bugs, race problems, race conditions, exploits
Technological obsolescence	Antiquated or outdated technologies

Source: ©2008 ACM, Inc.

## Vulnerability Assessment

- Once you have identified the information assets of the organization and documented some threat assessment criteria, you can begin to review every information asset for each threat
- This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization
- Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset
- At the end of the risk identification process, a list of assets and their vulnerabilities has been developed
- This list serves as the starting point for the next step in the risk management process: risk assessment

## Risk Assessment

- The goal at this point is to create a method to evaluate the relative risk of each listed vulnerability

## Risk Identification Estimate Factors

### Risk is

The **likelihood** of the occurrence of a **vulnerability**

*Multiplied by*

The **value of the information asset**

*Minus*

The **percentage of risk mitigated by current controls**

*Plus*

The **uncertainty of current knowledge of the vulnerability**

## Likelihood

- Likelihood is the overall rating—often a numerical value on a defined scale (such as 0.1 – 1.0)—of the probability that a specific vulnerability will be exploited
- Using the information documented during the risk identification process, you can assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc.

## Assessing Potential Loss

- To be effective, the likelihood values must be assigned by asking:
  - Which threats present a danger to this organization's assets in the given environment?
  - Which threats represent the most danger to the organization's information?
  - How much would it cost to recover from a successful attack?
  - Which threats would require the greatest expenditure to prevent?
  - Which of the aforementioned questions is the most important to the protection of information from threats within this organization?

## Percentage of Risk Mitigated by Current Controls

- If a vulnerability is fully managed by an existing control, it can be set aside
- If it is partially controlled, estimate what percentage of the vulnerability has been controlled

## Uncertainty

- It is not possible to know everything about every vulnerability
- The degree to which a current control can reduce risk is also subject to estimation error
- Uncertainty is an estimate made by the manager using judgment and experience

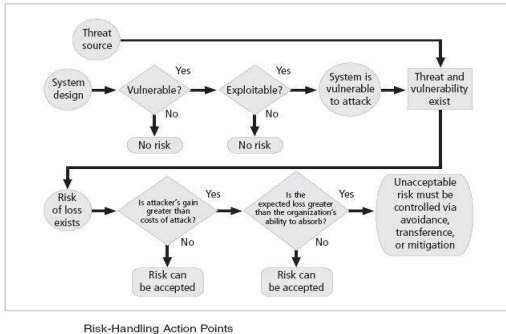
## Risk Control Strategies

- An organization must choose one of four basic strategies to control risks
  - **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 accepting the risk without control or mitigation

## Risk Control Strategy Selection

- Risk control involves selecting one of the four risk control strategies for the vulnerabilities present within the organization
- 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, the organization may choose to accept the risk
- Otherwise, one of the other control strategies will have to be selected

## Risk Handling Action Points

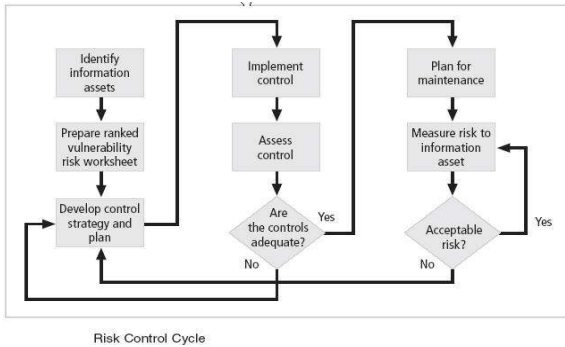


## Risk Control Strategy Selection

### Some rules of thumb:

- 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

## Risk Control Cycle



## Managing Risk

- Risk appetite (also known as risk tolerance) 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
- The reasoned approach to risk is one that balances the expense (in terms of finance and the usability of information assets) against the possible losses if exploited

## Evaluation, Assessment, and Maintenance of Risk Controls

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

## Feasibility Studies and Cost Benefit Analysis

- Before deciding on the strategy for a specific vulnerability, all readily accessible information about the consequences of the vulnerability must be explored
  - "What are the advantages of implementing a control as opposed to the disadvantages of implementing the control?"
- There are a number of ways to determine the advantage or disadvantage of a specific control
- The primary means are based on the value of the information assets that it is designed to protect

## Cost Benefit Analysis (CBA)

- The criterion most commonly used when evaluating a project that implements information security controls and safeguards is economic feasibility
- Organizations are urged to begin a cost benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised
- This decision-making process is called a cost benefit analysis or an economic feasibility study

## Cost

- Just as it is difficult to determine the value of information, it is difficult 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
- The benefit is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk there is for the asset
- This is expressed as the **Annualized Loss Expectancy (ALE)**

## Asset Valuation

- Asset valuation is the process of assigning financial value or worth to each information asset
- The value of information differs within organizations and between organizations, based on the characteristics of information and the perceived value of that information
- The valuation of assets involves estimation of real and perceived costs associated with the 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

- An organization must be able to place a dollar value on each information asset 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

- A Single Loss Expectancy, or SLE, is the calculation of the value associated with the most likely loss from an attack
- SLE is a calculation based on the value of the asset and the expected percentage of loss that would occur from a particular attack:

$$\text{SLE} = \text{asset value (AV)} \times \text{exposure factor (EF)}$$

Where EF = the percentage loss that would occur from a given vulnerability being exploited

- This information is usually estimated

## Asset Valuation Techniques (continued)

- In most cases, the probability of a threat occurring is the probability of loss from an attack within a given time frame
- This value is commonly referred to as the ARO, or Annualized Rate of Occurrence

$$\text{ALE} = \text{SLE} * \text{ARO}$$

## 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 calculated after controls have been implemented and have been functioning for a time:

$$\text{CBA} = \text{ALE}(\text{prior}) - \text{ALE}(\text{post}) - \text{ACS}$$

- 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

## Exposure Factor (EF) Example

- A primary e-Commerce web server is compromised and becomes unavailable
- The server is valued at \$5000
- The EF is deemed to be 75%

## Single Loss Expectancy (SLE) Example

- $\text{SLE} = \text{Asset Value (\$)} \times \text{EF}$
- The server is worth \$5000 &  $\text{EF} = 75\%$
- $\text{SLE} = \$5000 \times .75 = \$3750$
- The cost for a single occurrence of the web site being unavailable is \$3750

## Annualized Rate of Occurrence (ARO)

- The ARO has been estimated to be **three times per year** based on types of vulnerabilities and threats that are known and documented that relate to the type of server.

## Annualized Loss Expectancy (ALE) Example

- $ALE = SLE \times ARO$
- SLE is \$3750
- ARO is estimated @ 3 times per year
- $SLE = \$3750 \times 3$
  
- The Annualized Loss Expectancy relating to this server is \$11,250

## Cost Benefit Analysis (CBA)

- Control Strategy selected is to reduce web server vulnerability → **Avoidance**
- InfoSec investment / expense → Install a firewall with intrusion detection system (IDS)
- The Firewall / IDS installed is estimated to cost \$ 7500 per year (lease with service contract)
- Annual Cost of Safeguard is \$ 7,500

## Cost Benefit Analysis (CBA) cont.

- ALE (prior) is \$ 11,250
- The Control / Safeguard is estimated to reduce identified vulnerabilities by 80%
- $ALE (post) = \$11,250 \times .20 = \$2,250$
- $CBA = ALE (prior) - ALE (post) - ACS$
- $CBA = \$11,250 - \$2,250 - \$7,500$
- $CBA = \$1500$

## Cost Benefit Analysis (CBA)

- A \$7,500 annual expense yields
- A \$1,500 annual cost savings

A 20% Information Security Solution Return on Investment

## References

- Management of Information Security, 2<sup>nd</sup> Ed.  
Whitman and Mattord, Course Technology  
ISBN: 1-4239-0130-4
- Calculating Security ROI is Tricky Business  
Marcia Wilson, *Computerworld*, July 2003
- Measuring the Risk-Based Value of IT Security Solutions  
Arora, et. al., *IT Pro*, Nov | Dec 2004, IEEE