

IT 4823

Information Security Administration

Risk Assessment and Management



Notice: This session is
being recorded.

Risk Management

You've read most of this in the chapter.

This is a more organized form, I hope.

This lecture is taken from *Information Security is Information Risk Management* by Blakley, McDermott and Geer.

Threats and Risks

- A *threat* is something bad that can happen. In our case, something bad that can happen to an information asset.
- A *risk* is the probability that a particular threat to a particular asset will occur.

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 organizations data and information systems

Information Risk

- Use of information technology creates risk to
 - Confidentiality
 - Integrity
 - Availabilityof information assets
- Risk may be direct (to the asset itself)
- Or indirect (business interruption, damage to reputation, legal liability, etc.)

Quantifying Risk

Two related measures:

- Single loss exposure (SLE)
- Annualized loss expectation (ALE)

Single Loss Exposure

- The single loss exposure (SLE) of an adverse event is the cost incurred if the event takes place.
- It may be a range. Example: the SLE of an automobile wreck (for the car only) may range from a couple of thousand dollars to a “totaled” car, the entire cost.

Annualized Loss Expectation

- Probability of event occurring in one year times economic impact (SLE).
- The *actual cost* is either zero or the full economic impact.
- A good ALE depends on good estimates of both probability and cost.
- For large numbers (*e.g.* car insurance) this can be a quite precise actuarial estimate.
- ALE can be a range.

Measuring Risk

- Risk is the probability of an event that would reduce the value of a business asset were it to occur.
- Adverse events have costs (SLE) if they occur
- Risks are probabilities: annual rate of occurrence (ARO)
- The “cost” of a risk is the probability that the adverse event will be realized times the economic impact if it is. This is “annualized loss expectation.” $ALE = SLE \times ARO$

Cost Benefit Analysis

- The most common approach for information security controls is economic feasibility of implementation
- Cost benefit analysis (CBA) is begun by evaluating worth of assets to be protected and the loss in value if those assets are compromised
- The formal process to document this is called cost benefit analysis or economic feasibility study

Elements of Cost of Controls

- Cost of purchase or development;
- Training cost;
- Implementation cost;
- Cost of maintenance and operation.

Cost-Benefit Analysis

- Conduct to determine appropriate controls
 - greatest benefit given resources available
- Qualitative or quantitative
- Justify cost by a reduction in risk
- Contrast impact of implementing it or not
- Fundamentally a business decision
- Management chooses selection of controls
- Considerations: sufficient risk reduction, is too costly, or appropriate

Cost Benefit Analysis

- The “benefit” is the value an organization realizes by using controls to reduce the risks associated with a vulnerability
- Asset valuation is process of assigning financial value or worth to each information asset; there are many components to asset valuation

Cost Benefit Analysis

- Once value of various assets is estimated, potential loss from exploitation of vulnerability is examined
- This process results in an estimate of potential loss per risk
- Expected loss per risk is stated in the following equation:

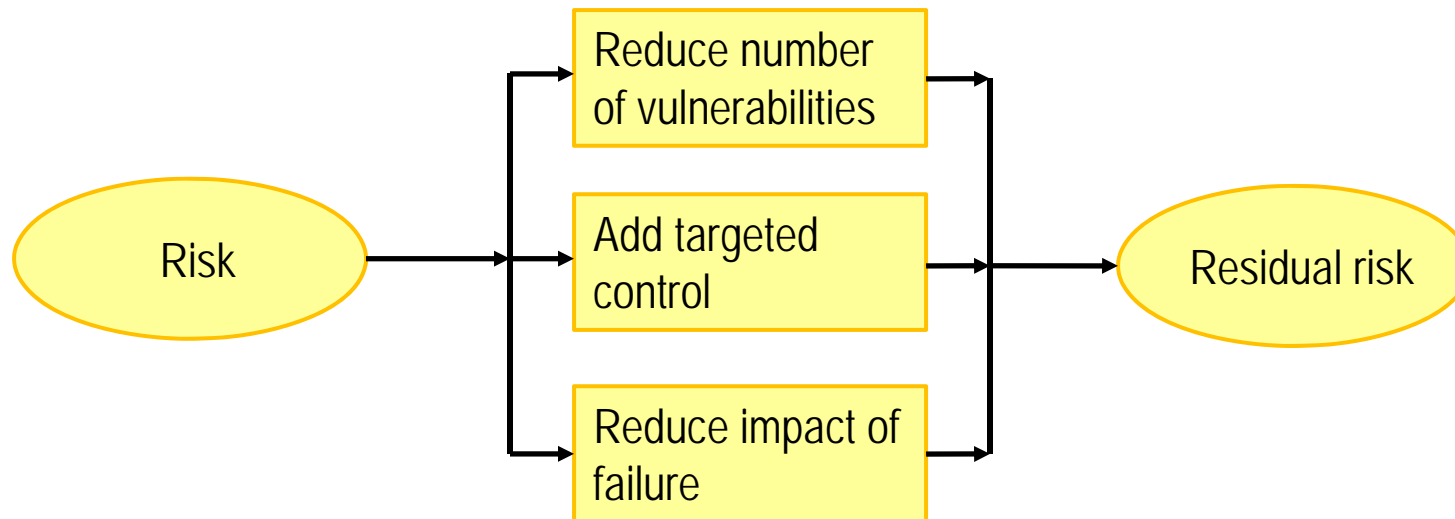
Annualized loss expectancy (ALE) equals
Single loss exposure (SLE) \times Annualized rate of
occurrence (ARO, probability of loss)

The Cost Benefit Analysis Formula

- $ALE = \text{Annualized Loss Expectation}$
- $ACC = \text{Annual Cost of Control}$
- $B = ALE(\text{before}) - ALE(\text{after}) - ACC$
- If B (benefit) is positive, it makes financial sense to implement the control.

Residual Risk

Risk remaining after controls are in place.
(Risk is never zero.)



Example

- A networked system has 100 workstations and 100 users, each of whom earns (on average) \$20/hour. The \$20 is “fully burdened.”
- The probability of malicious software being introduced into the network in a single year is 95%.
- Cleaning malicious software is assumed to take three hours.
- Antivirus software costs \$25 per workstation.
- Antivirus software will prevent 98% of malicious software infections.

Example Continued

- $SLE = \$20 \times 100 \times 3 = \$6,000$
- $ARO(\text{before}) = 0.95$
- $ALE(\text{before}) = \$6,000 \times 0.95 = \5700
- $ARO(\text{after}) = 0.95 \times 0.02 = 0.019$
- $ALE(\text{after}) = \$6,000 \times 0.019 = \114
- $ACC = \$2,500$
- $B = 5,700 - 114 - 2500 = \$3,086$
- Conclusion: Install antivirus!

Example: Challenging the Numbers

- The \$20 can be very accurate.
- 95% risk of infection: estimated by a security practitioner; may be too low.
- Antivirus software intercepts 98% of malicious software: from research on a sample of malware.
http://www.av-comparatives.org/images/stories/test/ondret/avc_report25.pdf
- Cost of installation, training, maintenance not included.
- Potential impact on performance not included.

Managing Risk

There are several ways to manage risk:

- Liability transfer
- Indemnification
- Mitigation
- Retention

Liability Transfer

- Accomplished by disclaiming risk, making it “someone else’s problem.”
- This can be by a disclaimer, a limited warranty, or a written agreement.

Indemnification

- Risk pooling (insurance)
- Hedging: a bet that an adverse event will happen.
(Consider financial securities hedging.)
A “hot site” is a kind of hedge.

Mitigation

- Reduce the expected cost by reducing the probability that the adverse event will occur. (Lock the doors.)
- Reduce the expected cost by limiting the damage if the adverse event does occur. (Keep valuables in a bank deposit box.)

Retention

- Self-insurance: setting aside funds to cover the risk
- Acceptance: accepting the risk without specifically setting aside funds.
- Definition: **residual risk**. Risk that remains after risk management. (Like the deductible on an insurance policy.)

Asset 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

Asset Identification and Valuation

- Iterative process; begins with identification of assets, including all elements of an organization's system (people, procedures, data and information, software, hardware, networking)
- Assets are then classified and categorized

Data Asset Identification

Asset attributes for data classification:

- Owner/creator/manager;
- Data structure size;
- Data structure used;
- Online/offline;
- Location;
- Backup procedures employed

Hardware, Software, and Network Asset Identification

- What information attributes to track depends on:
 - Needs of organization/risk management efforts
 - Management needs of information security/information technology communities
- Asset attributes to be considered are: name, asset type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity

Threat Identification

- Realistic threats need investigation; unimportant threats are set aside
- Threat assessment:
 - Which threats present danger to assets?
 - Which threats represent the most danger to information?
 - How much would it cost to recover from event?
 - Which threat requires greatest expenditure to mitigate?

Vulnerability Identification

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities
- Examine how each threat could be perpetrated and list organization's assets and vulnerabilities

Vulnerability Identification

- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions
- At end of risk identification process, list of assets and their vulnerabilities is achieved

Policy

- Who shall be allowed to do what.
 - Mandatory
 - Permissible
 - Prohibited
- Policy defines controls
 - Business processes
 - Technical measures
- Policy is the foundation of risk management (just like the rest of information security.)

Controls

- Protective measures
- Detection
- Response
- Assurance

Controls or Safeguards

- Controls or safeguards are:
 - practices, procedures or mechanisms which may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recovery
- Classes of controls:
 - Management
 - Operational
 - Technical
- Compare to McCumber Model: Policy, education, technology

Lists of Controls

CLASS	CONTROL FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

Focus and Bias

- Current information security focuses primarily on mitigation.
- There is a bias toward technological mechanisms
- There is a bias in favor of logical rather than physical mechanisms

Effectiveness

- Nearly 100% of companies in a 2000 survey by the FBI employ some information security mechanisms: antivirus, firewall, access control, etc.
- Losses due to information security failures are increasing.
- Conclusion: the methods employed are not effective

Quantification

- Most information security risk assessments are qualitative, low/medium/high, with respect to both probability and cost (and that's how the textbook presents it.)
- Good data are necessary to quantify both probability and cost.
- Good data are lacking

Areas to Measure

- Vulnerabilities:
 - No good taxonomy exists.
 - Reporting vulnerabilities may invite exploitation (but security by obscurity doesn't work, either)
- Incidents, with relation to vulnerabilities
- Losses
- Effectiveness of security controls

The State of Information Security

- Similar to medicine in the 19th Century
- A large selection of “cures” but very little data.
- Improvements in medicine are based on quantitative data. (“Evidence-based medicine.”)
 - Licensure
 - Systematic collection of public health data
 - Systematic studies of effectiveness

Physicians

- A specialized education
- A revocable license to practice
- An ethical obligation to treat patients appropriately
- An ethical obligation to keep patients' confidences
- A professional obligation to control potentially harmful treatments
- A professional obligation to report public health information

Information Security Specialists

- Little specific formal education or training; specifically, no training in experimental design.
- No licensure
- Ethical obligations embodied in codes of ethics of (voluntary) professional organizations.
- No obligation to assess costs and benefits
- Voluntary reporting and small samples

Summary: We Need...

- More and better data collection
- Serious attempts to quantify both probabilities and costs of risks
- Focus on policy
- Use of controls other than mitigation: transfer, indemnification, retention
- Acceptance of process and physical controls.

Questions

