



Minnesota State Colleges & Universities

# Security Risk Assessment

*Applied Risk Management*

July 2002

Information Technology Services

Minnesota State Colleges and Universities

# What is Risk?

Risk is:

- Something that creates a hazard
- A cost of doing business

*Risk can never be eliminated, merely reduced to an acceptable level*

# Risk Management

*Allocation of resources based upon informed choice*

To manage risk you must:

- Understand what must be protected
- Understand the hostile environment
- Understand the limits of your control
- Understand the consequences

*Risk can then be quantified, prioritized, and lowered to an acceptable level*

# The Elements of Risk

Risk includes the following three elements:

- Asset: the entity requiring protection
- Threat: the event creating the hostile environment
- Vulnerability: a deficiency creating the hazard

( Assets may have multiple threats *and* vulnerabilities )

*Threats exploit vulnerabilities to harm an asset*

# The Security Domain

*The security domain defines limits to organizational control*

## The Security Domain:

- Is defined by physical and logical perimeter boundaries
  - Physical walls and fences
  - External router/firewall interfaces
- Includes assets that are by definition controllable
- Establishes scope of Threat Analysis

# Risk Strategies

Risk may be:

- Mitigated by the deployment of countermeasures
- Transferred via insurance or assignment
- Accepted when the cost of protection exceeds harm

*Strategy selection is based upon Cost Benefit Analysis*

# The Security Risk Assessment

## *Applied Risk Management*

The Security Risk Assessment is:

- *A method to identify and understand limits to organizational control (scope)*
- *A tool to identify organizational assets, threats, and vulnerabilities (threat analysis)*
- *A process to quantify hazards based upon probability and harm (risk prioritization)*
- *A means to justify risk management strategies and allocation of assets (cost benefit analysis)*

# Risk Assessment Process

- Define Security Domain
- Identify assets
- Identify threats
- Identify vulnerabilities
- Determine probability
- Determine harm
- Calculate risk

*Risk may now be managed*

# Assets

*That which is of value to the organization*

## Tangible Assets

- *Buildings*
- *Employees*
- *Data processing equipment*

## Intangible Assets

- *Intellectual property*
- *Goodwill*

# Threats

*Realistic events with potential harm*

## Natural Threats

- *Acts of God*

## Accidental Threats

- *Worker Illness*
- *Equipment Failure*

## Intentional Threats

- *Asset Theft*
- *Asset Tampering*

# Vulnerabilities

*The chinks in the armor*

Vulnerabilities may be found in:

- *Location*
- *Skills*
- *Continuity planning*
- *Access controls*
- *Network monitoring*

# Probability

*Frequency in which threat will exploit vulnerability independent of harm*

Probability of each asset/threat/vulnerability combination should be quantified

Probability	Definition	Scale
<i>Negligible</i>	<i>Unlikely to occur</i>	<i>0</i>
<i>Very Low</i>	<i>2-3 times every 5 years</i>	<i>1</i>
<i>Low</i>	<i>&lt;= once per year</i>	<i>2</i>
<i>Medium</i>	<i>&lt;= once every 6 months</i>	<i>3</i>
<i>High</i>	<i>&lt;= once per month</i>	<i>4</i>
<i>Very High</i>	<i>=&gt; once per month</i>	<i>5</i>
<i>Extreme</i>	<i>=&gt; once per day</i>	<i>6</i>

# Harm

*Impact if threat exploits vulnerability independent of probability*

Harm of each asset/threat/vulnerability combination should be quantified

Harm	Definition	Scale
<i>Insignificant</i>	<i>No impact</i>	<i>0</i>
<i>Minor</i>	<i>No extra effort required to repair</i>	<i>1</i>
<i>Significant</i>	<i>Tangible harm / extra effort required to repair</i>	<i>2</i>
<i>Damaging</i>	<i>Significant expenditure of resources required Damage to reputation and confidence</i>	<i>3</i>
<i>Serious</i>	<i>Extended outage and / or loss of connectivity Compromise of large amounts of data or service</i>	<i>4</i>
<i>Grave</i>	<i>Permanent shutdown Complete compromise</i>	<i>5</i>

# Risk = Probability X Harm

*Quantification based on both frequency and impact*

Risk of each asset/threat/vulnerability combination should be calculated

Scale	Definition
<i>0</i>	<i>NIL</i>
<i>1-3</i>	<i>Low</i>
<i>4-7</i>	<i>Medium</i>
<i>8-14</i>	<i>High</i>
<i>15-19</i>	<i>Critical</i>
<i>20-30</i>	<i>Extreme</i>

# Example Matrix

Asset	Threat	Vulnerability	Prob	Harm	Risk	Control
Data Center	flood	Proximity to river	0	5	NIL	Not in 100 year flood plain
System Administrator	Absence	Lack of cross training	4	2	HIGH	No funding. Risk accepted
Web Server	Disk crash	Insufficient backup	2	3	MEDIUM	Daily data backup. Spare hardware onsite
Research work	theft	Communication channel security	1	4	MEDIUM	Data Protection Standard requires encryption for external communications.
Organization Reputation	Server unavailability	External internet interfaces	5	4	EXTREME	DDoS filters enabled on all external interfaces

# Benefits

The Security Risk Assessment will:

- Clarify the limits of control
- Quantify the threat environment
- Prioritize and justify business decisions
- Document due diligence