Security Risk Management

Identifying and Mitigating Threats To Your Bottom-Line
Topics

- Typical Security Risks
- Identifying Threats
- Evaluating Security System Effectiveness
- Risk Management
Typical Security Risks

- Theft
- Litigation
- Business Continuity
Security Risks: Theft

- **Product/Materials/Supplies**
  - Costs = (Labor + Material + Shipping + Insurance + Profit) x 2
  - Damage to Reputation

- **Information**
  - Costs = Market Share, Competitive Advantage, etc.
Security Risks: Litigation

- Customers/Employees
  - Workplace Violence
  - Inadequate Security

- Costs
  - Defense
  - Settlements
  - Damage to Reputation
Security Risks: Business Continuity

- **Natural Disaster**
  - Proactive planning limits loss time

- **Sabotage**
  - Damage to facilities
  - Injury to personnel
  - Loss of product/materials
Definition: Security Risk

A **Security Risk** is the probability of sustaining a loss of a specific magnitude during a specific time period due to a failure of security systems.
Risk Equation

\[
\text{Risk} = P_O \times C \times (1-P_W)
\]

\(P_O\) = Probability of Occurrence
\(C\) = Consequence Value
\(P_W\) = Probability of System Win (Effectiveness)
PO = Probability of Occurrence

Key Question:
What is the likelihood of this type of action occurring?

Key Question:
How can I develop an estimate?

- Company records
- Industry experience
C = Consequence Value

- The relative impact on the business if the action is successful
- Different set of values for each type of action
- Values range:
  - 0.0 = No impact/consequence
  - 1.0 = Very significant impact
\[ P_W = \text{Probability of System Win} \]

(Effectiveness)

Three components:

- Detection
- Neutralization
- Response
Identifying Threats

Key Question:
Who are the threats?

- Outside
- Inside
- Inside/Outside Collusion
Identifying Threats: Outside

- Common Criminals
- Organized Criminals
- Psychologically Unstable Individuals
- Competitors
  - Foreign
  - Domestic
- Terrorists
Identifying Threats: Inside

- Employees
- Vendors
- Contractors
- Temporary Employees
Threats

Key Question:
Why would my company be targeted?
Why My Company??

- High Value Materials
  - Product
  - Components
  - Tools
- Perception of Indifference
  - “Management doesn’t care”
Why My Company?

- Competitive Advantage
  - New Products
  - Market Strategy
- Political Incorrectness
  - Animal Research/"Exploitation"
  - Bio/Environmental Hazards
Why My Company?

- Disgruntled Employees
  - Labor/Management Issues
  - Poor Morale
  - Downsizing
- “Deep Pocket” Theory of Litigation
  - Somebody has to be responsible for .......
Evaluating Security System Effectiveness

- Define Security System Features
- Determine System Effectiveness
Define Security System Features

- Conduct a physical security audit
  - Barriers
  - Locks
  - Alarms
  - Communications
  - Response Times/Procedures
Define Security System Features

- Review access control process
- Review security policies/procedures
Define Security System Features

- Review access control process:
  - Who can gain access?
  - How do you handle:
    - visitors
    - vendors
    - temporary employees?
  - What are your key control procedures?
Define Security System Features

- Review security policies/procedures
  - Workplace violence issues
  - Document controls
  - Computer/network access
  - Background checks
  - Audits
Determine System Effectiveness

- Evaluate the security system from the adversary’s perspective

**Key Questions:**

1. How will the alarm be generated?
2. How long will the response take?
3. What form will the response take?
4. How much time will the adversary require?
Determine System Effectiveness

- Key questions have both Insider and Outsider dimensions
- Very Important to identify and differentiate system response
- A safeguard that works well for Outsiders, may not have the same effectiveness for Insiders
Risk Management

Three Choices:

- Accept
- Insure
- Mitigate

Reality is that you should use a combination of all three.
Risk Management

A CYCLICAL PROCESS

Identify Problems

Develop Solutions

Monitor Progress

Implement Changes
Accept

- Risks that are acceptably low
  - Probability of occurrence very infrequent
  - Low consequence

- Cost of Insuring or Mitigating unacceptably high
Insure

- Where possible at reasonable cost
- After mitigation
Mitigate

- All High Risk conditions
- Reduce consequences
  - Minimize exposures
  - Develop contingency plans
- Revise protection system
  - Improve access controls
  - Modify alarm systems
  - “Harden” targets
Decision Tools

- **Cost/Benefit**
  - Bottom-line approach
  - Weighs cost of alternative decisions against the benefits to be gained
  - Usually requires detailed estimates of future costs

- **Analytical Hierarchy**
Cost/Benefit

- Bottom-line approach
- Weighs cost of alternative decisions against the benefits to be gained
- Usually requires detailed estimates of future costs
Analytical Hierarchy

- Allows the use of a wider variety of parameters
- A series of paired choice decisions
Summary

- **Your** Company may be at RISK
- Identify
  - Threats
  - Consequences
  - Security Program Effectiveness
- Accept, Insure, or Mitigate
- Use accepted decision tools
Summary

- Develop risk management alternatives
- Implement decisions
- Monitor success
- Revise as necessary