Winning Initiatives and Best Practices for Physical Security
Today’s Presentation

1. Using a risk-based strategy for security
2. The balanced security approach
3. Concentric circles of protection concept
4. Good security vs. bad security
5. Common security mistakes
6. Questions and answers
Risk-Based Strategy for Security Planning
Traditional Approach to Planning Security

- Do what has always been done
- Do what everyone else is doing
- Reactive rather than proactive
- Always solving yesterday’s problems
Most facilities are spending lots of money on security, but can’t really tell you why.
If you don’t know your security risks, how can you apply the right security solutions?
Would you start taking medicines before your disease has been diagnosed?
Risk-Based Approach to Security
Risk-Based Approach to Planning Security

Premise:
Every security measure should be in response to one or more specific security risks
Risk-Based Approach Process

- Identify and prioritize your security risks
- Determine the best types of security measures to mitigate those risks
- Focus on high-priority risks first
- Deal with lower-priority risks as resources allow
Step #1 – Identify your assets

- People
- Property
- Infrastructure
- Information
- Reputation
Step #2 – Create a Risk Matrix

<table>
<thead>
<tr>
<th>Possible Loss Event</th>
<th>Likelihood</th>
<th>Consequences</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step #3 – Identify Possible Loss Events

- Arson
- Assault
- Burglary
- Disturbances/Disorderly Conduct
- External Theft
- Internal Theft
- Robbery
- Sabotage
- Theft of Employee Personal Property
- Theft of Information
- Disclosure of Trade Secrets
- Trespassers
- Vandalism
- Graffiti
- Workplace Violence
- Product Tampering
Step #4 – Determine Likelihood of Event

**Very Likely** = Greater than 90% chance of occurrence

**Likely** = Between 50% and 90% chance of occurrence

**Moderately Likely** = Between 10% and 50% chance of occurrence

**Unlikely** = Between 3% and 10% chance of occurrence

**Very Unlikely** = Less than 3% chance of occurrence
Step #5 – Determine Consequences of Events

**Not Serious** = No injuries, no downtime, $0 to $5,000 financial loss.

**Not Too Serious** = Minor injuries, less than 1 day of downtime. $5,000 to $50,000 financial loss.

**Serious** = Serious injuries, 1 to 7 days of downtime. $50,000 to $500,000 financial loss.

**Very Serious** = Loss of life or severe injuries, 7 to 30 days downtime. $500,000 to $1,000,000 financial loss.

**Catastrophic** = Loss of multiple lives or multiple severe injuries, significant or total destruction of facility, greater than $1,000,000 financial loss.
## Step #6 – Enter Data in Risk Matrix

<table>
<thead>
<tr>
<th>Possible Loss Event</th>
<th>Likelihood</th>
<th>Consequences</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arson</td>
<td>VU</td>
<td>VS</td>
<td></td>
</tr>
<tr>
<td>Assault</td>
<td>U</td>
<td>VS</td>
<td></td>
</tr>
<tr>
<td>Burglary(^1)</td>
<td>VL</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>Disturbances/Disorderly Conduct</td>
<td>U</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>External Theft</td>
<td>L</td>
<td>NTS</td>
<td></td>
</tr>
<tr>
<td>Internal Theft</td>
<td>VL</td>
<td>NTS</td>
<td></td>
</tr>
<tr>
<td>Robbery</td>
<td>VU</td>
<td>VS</td>
<td></td>
</tr>
<tr>
<td>Sabotage(^1)</td>
<td>VU</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Theft of Employee Personal Property</td>
<td>VL</td>
<td>NS</td>
<td></td>
</tr>
<tr>
<td>Theft of Information</td>
<td>L</td>
<td>VS</td>
<td></td>
</tr>
<tr>
<td>Disclosure of Trade Secrets</td>
<td>U</td>
<td>VS</td>
<td></td>
</tr>
<tr>
<td>Trespassers</td>
<td>ML</td>
<td>NS</td>
<td></td>
</tr>
<tr>
<td>Vandalism</td>
<td>U</td>
<td>NS</td>
<td></td>
</tr>
<tr>
<td>Workplace Violence</td>
<td>VU</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>Product Tampering</td>
<td>VU</td>
<td>VS</td>
<td></td>
</tr>
</tbody>
</table>
Step #7 – Rank Your Security Risks

Likelihood x Consequences =

Level of Security Risk
<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Very Likely</td>
<td>High Risk</td>
</tr>
<tr>
<td>Likely</td>
<td>High Risk</td>
</tr>
<tr>
<td>Moderately Likely</td>
<td>High Risk</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Moderate Risk</td>
</tr>
<tr>
<td>Very Unlikely</td>
<td>Moderate Risk</td>
</tr>
</tbody>
</table>
## Step #8 – List Rankings on Risk Matrix

<table>
<thead>
<tr>
<th>Possible Loss Event</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arson</td>
<td>VU</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Assault</td>
<td>U</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Burglary(^1)</td>
<td>VL</td>
<td>S</td>
<td>H</td>
</tr>
<tr>
<td>Disturbances/Disorderly Conduct</td>
<td>U</td>
<td>S</td>
<td>M</td>
</tr>
<tr>
<td>External Theft</td>
<td>L</td>
<td>NTS</td>
<td>M</td>
</tr>
<tr>
<td>Internal Theft</td>
<td>VL</td>
<td>NTS</td>
<td>M</td>
</tr>
<tr>
<td>Robbery</td>
<td>VU</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Sabotage(^1)</td>
<td>VU</td>
<td>C</td>
<td>M</td>
</tr>
<tr>
<td>Theft of Employee Personal Property</td>
<td>VL</td>
<td>NS</td>
<td>M</td>
</tr>
<tr>
<td>Theft of Information</td>
<td>L</td>
<td>VS</td>
<td>H</td>
</tr>
<tr>
<td>Disclosure of Trade Secrets</td>
<td>U</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Trespassers</td>
<td>ML</td>
<td>NS</td>
<td>L</td>
</tr>
<tr>
<td>Vandalism</td>
<td>U</td>
<td>NS</td>
<td>L</td>
</tr>
<tr>
<td>Workplace Violence</td>
<td>VU</td>
<td>S</td>
<td>L</td>
</tr>
<tr>
<td>Product Tampering</td>
<td>VU</td>
<td>VS</td>
<td>M</td>
</tr>
</tbody>
</table>
### Step #9 – Focus on High-Priority Risks First

<table>
<thead>
<tr>
<th>Possible Loss Event</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arson</td>
<td>VU</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Assault</td>
<td>U</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Burglary(^\d)</td>
<td>VL</td>
<td>S</td>
<td>H</td>
</tr>
<tr>
<td>Disturbances/Disorderly Conduct</td>
<td>U</td>
<td>S</td>
<td>M</td>
</tr>
<tr>
<td>External Theft</td>
<td>L</td>
<td>NTS</td>
<td>M</td>
</tr>
<tr>
<td>Internal Theft</td>
<td>VL</td>
<td>NTS</td>
<td>M</td>
</tr>
<tr>
<td>Robbery</td>
<td>VU</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Sabotage(^\d)</td>
<td>VU</td>
<td>C</td>
<td>M</td>
</tr>
<tr>
<td>Theft of Employee Personal Property</td>
<td>VL</td>
<td>NS</td>
<td>M</td>
</tr>
<tr>
<td>Theft of Information</td>
<td>L</td>
<td>VS</td>
<td>H</td>
</tr>
<tr>
<td>Disclosure of Trade Secrets</td>
<td>U</td>
<td>VS</td>
<td>M</td>
</tr>
<tr>
<td>Trespassers</td>
<td>ML</td>
<td>NS</td>
<td>L</td>
</tr>
<tr>
<td>Vandalism</td>
<td>U</td>
<td>NS</td>
<td>L</td>
</tr>
<tr>
<td>Workplace Violence</td>
<td>VU</td>
<td>S</td>
<td>L</td>
</tr>
<tr>
<td>Product Tampering</td>
<td>VU</td>
<td>VS</td>
<td>M</td>
</tr>
</tbody>
</table>
Step #10 – Determine Security Measures

Determine appropriate measures to mitigate each security risk
Security Risk
Theft of Information

Security Measures
Background checks
Employee training
Restricted access areas
High-security file cabinets
Document shredders
Security Risk
Burglary

Security Measures
High-security locks
Door frame strengthening
Security window film
Intrusion alarm system
Security patrols
Balanced Approach to Security
Good security is a process, not a product
Good security requires a balanced approach
Operational Measures

- Security policies and procedures
- Security management
- Employee awareness training
- Security officer staffing
- Incident investigation
Electronic Systems

- Access control systems
- Video surveillance systems
- Alarm systems
- Visitor management systems
- Security communications systems
Site and Building Design

- Site and facility layout
- Lighting
- Fencing and landscaping
- Doors and lock hardware
- Security signage
All elements must work together for effective security
Buying the equipment is the easy part........
Concentric Circles of Protection Concept
Concentric Circles of Protection

- Perimeter Fence
- Building Exterior
- Department Door
- Office Door
Layers of Security

Layer 1
Perimeter Fence

Layer 2
Exterior Wall

Layer 3
Lobby Wall

Layer 4
Department Wall

Layer 5
Office Wall

Layer 6
Safe

Layer 3
Lobby Wall
Concentric Circles of Protection Principles

- Having multiple layers decreases probability that intruder will be able to gain access
Concentric Circles of Protection Principles

- You can decrease intruder’s chance of success by...
  - ...adding layers
  - ...increasing the effectiveness of each layer...
- ...or by doing both
Concentric Circles of Protection Principles

- Relying on a single layer to provide security is almost never effective because it requires a level of perfection that is unattainable.
Concentric Circles of Protection Principles

- Simple procedures, such as the locking of file cabinets and offices, can provide additional security “layers” at little or no cost
Concentric Circles of Protection Principles

- Employee awareness can create an invisible, yet very effective, security “layer”
Good Security vs. Bad Security
Traits of a Good Security Program

- Operates based on a written plan that addresses identified security risks
- Employees know what is expected and why
- Losses and security incidents are minimized
- Employees and guests feel safe
- Facility is compliant with regulatory requirements
Traits of a Bad Security Program

- No cohesive security plan
- Program has been pieced together over the years in response to past problems
- Specific security risks have never been identified or prioritized
- Employees are unsure of what to do or why
- No real handle on what is happening at facility
Traits of a Bad Security Program

- Employees and guests don’t always feel safe
- People, property, and information may be at risk
- Facility may be non-compliant with regulatory requirements
- Potential for “negligent security” lawsuits
Common Security Mistakes
Not having or not following a written security plan
Not providing adequate security training to employees
Not keeping track of crimes occurring at your facilities
Not being aware of crimes being committed in the neighborhood
Not being responsive to employee complaints about security
Not alerting employees to known security risks
Cutting security measures just to save money
Thinking that security cameras are a “magic bullet”
Poor management and disposal of sensitive documents
Poor control of contractors and service providers
Poor background check procedures
Inadequate supervision of contract security services
Poor lighting
Poorly maintained security features
Not keeping up with changing conditions
Questions and Answers
Silva Consultants

Michael A. Silva, CPP
PO Box 8799
Covington, WA 98042 USA
Phone: 888-645-2299
Email: mikes@silvaconsultants.com
Website: www.silvaconsultants.com
(Lots of free security tips on website)