



Executive White Paper

November 2005

A Practical Guide to Business Security

Finding solutions to your facility security needs

Many businesses are driven to purchase security solutions after some form of incident. A purse is stolen, a computer vanishes or strangers are observed lurking around the property. It's quite natural for people to seek immediate remedies to restore their comfort level after such an event. Rather than responding to a single incident, it's important for business Managers to take this opportunity to assess their needs in a more holistic fashion.

While there is no substitute for obtaining professional risk assessment and security plan, it is possible to perform a preliminary self-assessment to determine which areas warrant your immediate focus

Start by creating a list of the types of incidents your business has experienced in the past 24 months. List the event along with the loss and the type of incident (Theft¹, Break-in², Vandalism, Workplace Violence³). Here is an example:

Date	Description	Actual Loss	Threat Type
10/04	Employee reported Purse stolen.	\$43.50	Theft
12/04	Employee found with customer database on memory stick	\$0	Theft
1/05	Warehouse reporting inventory variance.	\$1,940	Theft
3/05	Delivery person found unescorted in computer room.	\$0	Theft
6/05	Employee reported people lurking in parking lot.	\$0	Break-in, Workplace Violence
7/05	Employee reported desk change missing.	\$2.25	Theft
7/05	Doors left unlocked over Friday night.	\$0	Theft
10/05	Employee vehicle vandalized in parking lot.	\$300	Vandalism
11/05	Front window smashed, computer stolen.	\$1,500	Break-in, theft

Note:

- 1) For this example, theft is defined the loss of property to internal or external perpetrators.
- 2) For this example break-in is defined as forced intrusion, which can result in theft.
- 3) For this example workplace violence is defined as a physical attack or assault resulting in death or physical injury of an employee or customer in a place of business

It is important to list all security incidents; no matter how trivial they may seem or even if no loss was suffered. Certain types of incidents or a pattern of events could help a security expert uncover a problem that has not yet resulted in a loss to your business.

It is fairly common for thieves (internal and external) to probe your business looking for weaknesses or valuable targets prior to executing a theft. These probes will generally be very innocuous so as not to arouse suspicion. For example; an employee working late is discovered in a remote cubicle with a cover story that they were looking for office supplies. A courier is found in your facility claiming that they were called there for a pick-up.

Many businesses do not track or report security incidents where a material loss or physical harm does not occur. This can result in managers underestimating the risk to their businesses.

The Small Business Administration conducted a study (Fischer, 1997) of 400 small businesses and found that nearly 13 percent experienced at least one crime in a one-year period. The crimes occurred in the following order of frequency.

1. Burglary
2. Vandalism
3. Employee Theft
4. Motor vehicle theft/break-in
5. Employee assault

Every business is at some risk for these types of incidents. The probability of occurrence and consequences vary depending on a number of factors. Many security risk analysis programs use the formula $\text{Risk} = \text{Probability} \times \text{Consequences}$ to help weigh the relative importance of the various risks. If you don't feel comfortable assessing the potential risks to your business, there are several avenues that you can pursue:

1. Contact your local Police Department to determine if they have a business liaison program. If so, they may provide you with local crime statistics and perhaps a crime prevention survey of your property. Many Police Departments will also conduct employee awareness programs to help educate your workforce.
2. Purchase a self-assessment kit or obtain professional security assessment training. You can access information on these solutions by registering with Evaluweb (www.evaluweb.com) and using the Evalumatch engine or Supplier Gallery to locate appropriate providers.
3. Contact a security consultant who specializes in creating security risk assessments and mitigation plans. You can access information on these solutions by registering with Evaluweb (www.evaluweb.com) and using the Evalumatch engine or Supplier Gallery to locate appropriate providers.

Using our example above our business owner has created the following chart to help them prioritize the risks to their business

Threat	Probability	Consequence	Impact Rating
Theft	3	2	6
Break-in	1	2	3
Vandalism	2	1	2
Workplace Violence	1	3	3
Scale: Probability - 1 Unlikely, 2= Likely, 3= Very likely Consequences - 1= Modest, 2= Serious, 3= Very Serious			

From this analysis we conclude that the top security priority of this business is protection against theft.

Once you have completed a simple self-assessment and concluded which risks have the greatest impact for your business you can begin to investigate possible solutions. In general, your solutions will help do one or more of the following:

1. Decrease the probability of an incident occurring
2. Reduce the impact/severity of the incident
3. Enhance the recovery from an incident

Decreasing the probability of an incident can be accomplished by eliminating the precursors, by increasing the risk of being caught and by making the task more difficult. Here are some examples:

- Pre-screening employees can help you avoid hiring individuals with a history of criminal behavior.
- Limiting the movement of employees and visitors to designated areas with an access control system reduces the potential for unwanted behavior.
- The presence of closed circuit television (CCTV) cameras can discourage potential criminals who fear being caught.
- Fencing off, lighting and patrolling a parking area make it more difficult for criminals to enter and exit your property unnoticed.
- Maintain proper procedural controls and periodic inspections to discourage and reveal insider theft rings.

To reduce the impact and severity of an incident, shorten the time a criminal has to operate undetected, increase the difficulty of accessing valuable items and by hindering the criminal's escape. Here are some examples:

- An alarm system sounder will alert an intruder that they have been detected thus causing them to hasten or abandon their activities.
- Placing cash and valuables in a safe or locked room increases the time required to access them.
- Hire a guard service to conduct random tours of your property after business hours.
- Install a magnetic lock that sounds an alarm and delays the criminal's exit for a period of time. Thieves may drop their items and look for a quicker, quieter exit.

Since it isn't practical to deploy solutions that will prevent 100% of all incidents, it makes sense to organize response and recovery plans. You can increase your company's ability to recover from an incident by having back-up plans in place, by increasing your chance of recovering stolen items and by obtaining proper insurance against losses. Here are some examples:

- Maintain proper back-ups of critical business data in a highly secure location so that information can be restored in the hardware is stolen.
- Document and permanently mark all company assets to assist in recovery efforts.
- Formulate plans to communicate with employees and customers in the event of a serious incident.
- Use documentation from CCTV, Access Control and Alarm system to reconstruct the event and provide evidence to investigators.
- Obtain insurance against employee dishonesty, forgery, theft, robbery, destruction, extortion, computer fraud, guest liability, etc.

There are a variety of options available to a business owner to address their security risks. In many cases these solutions will be used in combination in order to best address the problem at the lowest total cost. Listed below are examples of how certain security solutions impact various types of threats.

Threat	Decrease Probability	Reduce Impact	Enhance Recovery
Theft	CCTV System Access Control Alarm System Asset Protection System ID Badging System Visitor Management Employee Screening Internal Controls	Alarm System Access Control Internal Controls	CCTV System Asset Tagging Data Back-up Insurance Communication Plan
Break-in	CCTV System Exterior Lighting Alarm System	Alarm System Access Control Guard Response	Insurance Communication Plan
Vandalism	CCTV System Guard Tour Physical Barriers	Alarm System Guard Response	Insurance Communication Plan
Workplace Violence	CCTV System Access Control Intercom System ID Badging System Visitor Management Employee Screening Employee Training	Panic Alarm Emergency System Access Control Employee Training	CCTV System Insurance Communication Plan Employee Training

To learn more about how each of these systems can help resolve security problems facing your business please view the Evaluweb white paper called the ABC's of Security on www.evaluweb.com. To view and compare systems in more detail, please become a member of Evaluweb and use the Evalumatch engine for your comparison.

Reference:

1. Bonnie Fisher, "Small Businesses, Big Burdens: The Nature and Incidence of Crime Within and Against Small Business and Its Customers and Employees, Their Causes, Their Effects, and Their Prevention" (1997) from US Small Business Administration
2. Workplace Violence: A Report to the Nation. University of Iowa Injury Prevention Research Center. Iowa City, Iowa: February 2001; Violence in the Workplace, 1993-1999. Special Report, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Washington, D.C.: December 2001, NCJ 190076
3. R.J Fischer and G. Green, Introduction to Security, 6th ed. Boston: Butterworth-Heinemann, 1998
4. James F. Broder, Risk Analysis and the Security Survey, 2nd ed. Boston: Butterworth-Heinemann, 2000

Synopsis

A Practical Guide to Business Security. Finding solutions to your facility security needs

Businesses face a variety of security risks every day. To find the most appropriate and cost-effective solutions for your business you have to conduct a risk assessment. Your risk assessment can be relatively simple or complex depending on the needs of your business. To start make a list the types of incidents which have or are likely to occur. Then rank each threat by probability of the occurrence and its consequences. Once you have calculated the priority of each risk you can evaluate how various solutions will help your business manage these risks.