SACS Consulting and Investigative Services
520 S. Main, Suite 2512
Akron OH 44311
1-888-722-7937
www.sacsconsulting.com

"We put you back in control of your workplace."

# THE CORPORATE SECURITY PLAN: REDUCING CORPORATE RISKS.

*David DiRocco, SACS Consulting and Investigative Service*

A proper security plan can do more than prevent criminal losses. When properly designed, a security plan reduces risks associated with violence, litigation, internal theft, and high insurance. It can help the organization comply with regulatory agencies, such as OSHA, BWC, and EEOC. And by making employees feel more secure, your security plan builds a positive corporate culture which improves productivity, safety compliance and quality of work. To achieve this, always remember:

1. The goal of a security program is not to catch bad guys. The goal is to protect the organization by reducing risks. At least 80% of security resources must be committed to prevention.
2. Absolute security is absolutely expensive and not a rational goal. Only after a thorough vulnerability assessment and risk analysis can you determine the logical extent of your security program.
3. Electronics and hardware are only a small part of the security plan. An HR based security policy and employee training are far more critical than locks, cameras, or alarms.
4. Outside contractors work for you. Make sure you keep control of them and that what they are selling you is in your best interest, not theirs.

## THE VULNERABILITY ASSESSMENT

Would you buy a piece of equipment without determining what function it performs? Or, hire an employee for whom you do not have a specific function? Unfortunately, that has been a traditional approach to security: alarms are installed, signs posted, and security guards hired without actually determining what function they should serve. This is where the vulnerability assessment becomes a valuable tool.

The function of the vulnerability assessment is to identify your organization's vulnerability to specific loss events. Also known as a security survey, the vulnerability assessment seeks to determine vulnerability to the 5 areas of your business:

1. Life and limb
2. Irreplaceable business documents (hard and electronic)
3. Assets (real and liquid)
4. Routine business documents (hard and electronic)
5. Business continuity

While the second through fifth areas may change depending on the type of business you run, life and limb is always number one! A thorough assessment takes into account potential violence against employees, visitors, vendors, and anyone else who enters your place of business.

## Risk Analysis

Once the vulnerability assessment has determined what to protect, a risk analysis needs to be performed to determine the risk of the specific loss events which have been identified. The risk is a function of three areas:

1. Threat: How likely is it that this loss event will occur?
2. Vulnerability: How likely is it that this event will be successful against our current countermeasures?
3. Consequence: What is the negative impact to the organization if this loss event occurs?

Remember when we said that infinite security is infinitely expensive? The risk analysis helps determine the allocation of resources by defining what assets should be protected and to what degree. While risk reduction is favorable, risks can also be avoided, assumed, spread or transferred. For example, the risk of fire can be *reduced* through prevention programs and *transferred* through insurance.

## The Security Program

The vulnerability assessment and risk analysis done, you now have an idea of *what* needs protected and *why*. Your security program will now spell out *how.*

Your security program should be a team approach. HR, legal counsel, facilities, operations, and corporate security should all be on the planning team. Do not forget to bring your insurance carrier in on the process. An underwriter can make recommendations which will result in lower insurance rates.

The program should start with HR based policy and procedure. It is very easy to get wrapped up in the latest technology, but the technology is no good without a policy governing use. Remember: hardware and electronics are a supplement to your program; they are not the program itself.

Many organizations choose to hire an independent security consulting firm to assist from the beginning. A security consultant can identify issues that are overlooked due to familiarity. They can often find problems that insiders may not bring up out of fear of reflecting poorly on a co-worker or

superior. A good security consulting firm should be able to provide references and be affiliated with a nationally recognized organization, such as the American Society of Industrial Security (ASIS).

Like your business, your security program is not a static product. Environmental change, business needs, political structure and time can change what is at risk and to what extent. Revisit your security program annually to determine if changes are needed.