Enhancing Office Security



Many of us live with a false sense of security. We think crime happens to other people and terrorism happens in other countries. Unfortunately, that's not true. Murders occur every 21 minutes and assaults every 16 seconds. This is especially true of the workplace. Office buildings in particular are common sites for criminal attacks of all kinds—by disgruntled workers, by perpetrators and victims of domestic violence and even by mentally impaired transients looking for a place to shack up.

"Security is an illusion. Life is either a daring adventure, or it is nothing at all."
—Helen Keller.

The reality is that we must consider all manner of threat to our personal safety, including in the workplace. Let's talk about ways to train office workers to pay attention to security.

Disarm Threats with Proactive Planning

An attacker's greatest weapon is the element of surprise. To act reactively is to be at the attacker's mercy. Eliminating surprise requires proactive behavior. As safety managers, you must take responsibility for workplace security. Premise security is typically the job of the in-house security officer; but they can't be everywhere at once. Here are some guidelines to help you eliminate common risks and enhance the security of your office or other workplace:

- Place barriers to access. Limit access to your facility to employees and authorized visitors. To keep everyone else out, enforce parking bans. Attackers often drive their vehicle right into the building where they commit their attacks. To reduce this risk, erect concrete highway dividers along your facility's perimeter. You can even use aesthetically pleasing barriers, such as flowerpots, concrete benches or sculptures.
- Remove trash containers. Remove trash barrels and waste bins in common areas near entranceways, both inside and outside, where trespassers might have access. Offices located near residential neighborhoods might find their trash bins overloaded with homeowner refuse that could be hazardous or even explosive.
- Secure ground floor vents. Street-level fresh air intake vents are designed to draw air for heating and cooling systems. But these vents pose bio-

terrorism risks. Protect your air supply from sabotage by fencing off moving vents or by moving them to higher levels. Ensure that inside and outside air passes through HEPA filters that remove all particles larger than 1 micron. You should also upgrade your smoke detection system to take advantage of new technology. Some smoke detectors can now sense carbon monoxide and even teargas, pepper spray and some nerve gas and chemical weapons.

- Reduce entry points. A single point of entry, whenever feasible, is best. It helps security personnel control who enters the building. You should also consider hiring guards trained to identify potential threats, rather than someone who just checks IDs. Pieces of paper with words and photos laminated in plastic are easy to counterfeit.
- Install security cameras. A security camera is your eye in the sky. You also need qualified people to "monitor the monitor." But remember that a single security guard watching 50 video screens won't cut it. At big facilities, the guard should be supported by trained and motivated plainclothes guards, inside and outside the facility, watching every aspect of your site at all times.
- Monitor shipping and receiving. This is a weak point in most security plans through which intruders can get in. In the shipping and receiving area, security personnel must:
    - Make sure no one enters the building; and
    - Check and scan all items before they enter the building.
- Monitor web use. Employees access the Internet at work for both job-related and personal activities. They may also use it for illegal activities. Alarmingly, the number of employees transmitting sensitive, proprietary company data via the Internet is increasing. If this is a concern in your organization, there are several surveillance technologies that can help your IT department monitor online activity. Many businesses use these techniques to protect their investments.

Conclusion

No matter what technologies and security methods you use, you should also have a third party conduct a security audit of your facility. An unbiased professional can spot security loopholes and vulnerabilities unique to your site, and make recommendations to help secure the future of your workplace, your employees and your business.