# Does Your Facility Have a Security Plan?

building OPERATING management

By Sean A. Ahrens SECURITY

OTHER PARTS OF THIS ARTICLE

**Pt. 1:** This Page

If you are responsible for security, you know how difficult it is to justify funding for security measures — until a security breach happens. At that point, senior management gets involved and one question will be asked: "What do you need to prevent this from happening again?" This is your opportunity to make the most of a security event and obtain the resources you need to be proactive to help avoid future events. If you are not prepared with a solid answer, the opportunity may be lost.

It is always worthwhile to be prepared to explain what resources you need to address security risks. Even if a security breach doesn't occur, having information ready can help you justify needed measures. If an incident does happen, you probably won't have time to do all the homework required for a good security plan.

boardroom or during a crisis, there is one commonality — a plan. In fact, the security plan is similar to a playbook, which consists of a carefully considered series of actions to be implemented.

Remember the old philosophical question, "If a tree falls in the woods and no one is there to hear it, does it make a sound?" It's much the same with security. How would anyone know that a security program is effective without an occurrence to test it? For instance, how do you show that the camera installed over the door acted as a deterrent to the person who was contemplating a violent act if the act did not occur? The answer is simple. You can't.

That is one reason why budget justifications are challenging for security. Compounding the problem, is that security is a cost center and does not drive revenue. To top it off, security breaches are rare. It is easy for top executives to take security for granted, but complacency is a breeding ground for disaster.

### Step One: Analyze Risks

When developing a security plan, there are multiple vulnerabilities and specific threats to consider. Some threats are common to many organizations, and some are specific to a particular organization. These risks should be examined and quantified by answering questions such as these:

- How attractive is the organization as a target?
- What would be the direct and indirect impacts of a given incident?
- What is the probability of a security incident occurrence?

These questions can be answered by examining the capability and the intent of an aggressor.

Once the risks are identified, your organization can and should be benchmarked against peer organizations. Benchmarking may seem unnecessary if you are responsible for security, because most likely you have already voiced the possible risks to executive management, sometimes without lasting effect. But benchmarking can be a powerful tool to validate that risks are real, evident and should be mitigated.

## Step Two: Security Measures

The second and often most important component for plan development is the set of controls or measures used to prevent a security incident. Physical security controls/measures are grouped into three broad elements: operations, architecture and technology.

Properly implemented, these controls can establish a balanced security program. Selecting and implementing the proper controls can be difficult. Ideally, when considering security measures, the assessment should look from outside the asset inward. One effective approach is to examine vulnerabilities from the perspective of an aggressor.

Examples of how an outside-in approach has been used to identify common lapses in security include the following:

***Physical Security:*** A facility typically appears more secure during the day than in the evening. Any determined aggressor will not want to be observed;

Lighting is the number one opportunity to discourage crime because a criminal's ultimate deterrent is the potential that bystanders will witness their act.

The breach of a building's perimeter is often much like the practice of magic, which utilizes diversion and movements that are not easily detected. Trying gain entry through seldom-used pedestrian entrances is illogical because the criminal may be more likely to be detected by occupants who expect only specific individuals to use that entrance. A better method may be to use the front door, where many people access the facility.

Another opportunity to mitigate crime is to introduce a defined perimeter through the use of soft barriers (landscaping) and defined/hard barriers (fencing). These create exclusionary zones, where an intruder would, in these areas, be more readily identified.

Criminals may also attempt to access a building through latch manipulation and lock picking. To deter physical access to a door, three elements are needed: Industrial locking hardware with high-security key-ways, pinned or concealed hinges and latch cover plates. The latch cover plate tends to be the most commonly overlooked element of the three; its absence allows an intruder to manipulate the door latch to gain entry.

***Technical Security:*** The first alarm system was patented by August Pope in 1853. It consisted of magnetic contacts that could be placed on doors and windows and would transmit their position as either open or closed. Even today, all technical alarms still need the same three basic components: a triggering device (commonly referred to as the sensor); a circuit (typically in annunciator or sounder that signals the alarm.

The alarm system has only one goal: Reduce the need for staff. But technology can only be effective if it is used properly. For example, an infant abduction system in the security control center of a hospital alarmed, indicating that an infant had been abducted. The officer in the control center did not respond. When asked why, he explained the alarm had been broken for weeks. In effect, the officer had been conditioned that all alarms were false.

The sophistication of security technology has come a long way, but technology can be defeated. Take the case of a man who repossessed cars. On one occasion, he came across a vehicle armed with ultrasonic, glass break and volumetric/seismic detection sensors within the car. It was a very robust system, which alarmed instantaneously when the vehicle was approached. Where others may have hidden their vehicles, the owner of this vehicle put his car out in the open. He, like many organizations, had fully invested in the technology and was confident that nobody could steal or repossess his vehicle.

The alarm system had one fault — false alarms, and a lot of them. So the man trying to repossess the car spent two hours late one evening repeatedly setting off the alarm. Finally, the person who owned the car stomped outside, flung the door open and disarmed the car alarm in order to get a full night of sleep. He was subsequently deprived of his car.

This story has several lessons: 1. Technology needs to be proven, and bleeding-edge technology may not be effective. 2. Technical alarm systems insignificant, need to be investigated. 4. Finally, an organization cannot completely rely on technology for its security program; to do so opens up a gaping hole that is easily exploited.

***Operational Security:*** Operational security represents the most common type of security and, when properly implemented, is often the most effective. A well-trained and properly documented security staff that is loyal to the goals and objectives of an organization does not come cheap.

Operational security is more than just staff; it is comprised of policies, procedures and guidance regarding the management of incidents. Operational security, in many cases, can be undermined by executives or staff who may feel hassled by security officers. Over time, the negativity can affect the attitude of the security staff, and security assumes a concierge role.

As an example, during an after-hours assessment of a facility with a single security position prominently located within the building's pedestrian common travel path, the officer on duty always greeted the security consultants as they moved within the facility. Just before leaving, one consultant said, "You have no idea who we are, do you?" The officer responded, "Nope." The officer, in effect, was an overpriced receptionist.

Operational security represents the weakest link and needs to be reviewed often. In one case, a hospital had established a policy that deemed the pediatric floor to be a high-security area that was to be staffed with three officers at all times. In reality, there were no officers on the pediatrics floor for long stretches of time — even though a security incident had just occurred.

Organizations need to empower employees to help ensure the security of their building. In many instances, gaining access to a facility is as simple as smiling and asking pleasantly, "Please hold the door for me." Organizations need to have broad-based security awareness programs that reach all employees which, done right, requires a significant expenditure.

## Step Three: The Playbook

Once the security measures have been identified using the outside-in approach, the next step is to put them together in a security playbook, or master plan, which shows accurate budgeting for the controls and measures being proposed. The planning should adopt a holistic, all-security-risks approach. In some instances, budgeting can be shared among additional corporate functions such as information technology or human resources. Budgeting should be phased and comprehensive. Rather than asking for $4 million at one time, highlight the risks and phase the implementation.

Another way to justify security measures is to show return on investment, which typically involves not only the return on technology investments, but highlights training programs, empirical reduction in incidents, etc.

Although it may not be seen, the playbook needs to be well written as there is a chance senior management will ask to see it. If it is not available to be presented immediately, the implementation of the plan could be delayed.

In addition, the plan needs to keep its audience in mind. Executives tend to either be spontaneous or cautious and detailed. To be on the safe side, both personalities should be kept in mind as the security plan is developed to ensure its support on the executive level.

This is a living document that needs to be updated regularly and will form the basis for any presentation to management. In anticipation of that occurrence, it is important to identify and meet with key stakeholders. The goal of this meeting is not to push an agenda, but to make others aware of resources in the spirit of building collaboration.

The statistical reality is that any organization, no matter size or type, will experience a security incident at some point. The more employees and the longer the organization exists, the greater the statistical probability of a security event. Embracing the need for a well thought-out security playbook can make the difference in obtaining resources once a security event occurs. Rather than sending endless emails about an organization's risk, be prepared so if a question about security needs comes from management, your response will be, "I have a plan. This is what we need to do, this is what it will cost, this is what we will gain."

*Sean A. Ahrens (sean.ahrens@aon.com), CPP, BSCP, CSC, is a project manager with Aon Risk Solutions' Global Risk Consulting practice. With more than eighteen years of experience in the security industry, Ahrens is responsible for providing organizational security consultation, threat and risk analysis, contingency planning, loss prevention and force protection design and planning.*

Contact FacilitiesNet Editorial Staff »

**0 Comments**

Sort by Oldest

Add a comment...

Facebook Comments Plugin