SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Policy and Guidelines >

Physical Security: Assessing the Needs of Your Business

By the Security Executive Council

The following is an excerpt from the Security Executive Council's Physical Security Strategy and Process Playbook publication. For more information about the full guideline, email us at contact@secleader.com

Physical security must make sense within the context of your business operations. In order to build a security system that works for any business, the needs of that business must first be assessed.

At the core of this assessment are the following operational issues:

- What is the general level of risk for this business?
- What are the critical events that will stop this business?
- What are the products, information, and assets at this site? What specific risks are associated with each of them?
- How do people and materials enter and leave?
- What are the work schedules?

We often recommend a security assessment as a means of identifying security issues relating to your business operations – your people, information, property, product, and the corporation's reputation.

In order to use a security assessment properly, you first need to understand the three fundamental elements of security: probability, criticality, and vulnerability.

Elements of Security

An effective security assessment applies an understanding of the fundamental elements of security to a particular location or area within the business.

As you look at each area, consider the following questions:

- What is the probability of a security-related incident occurring in this area?
- How critical might the incident be to my business operations?
- How vulnerable is the area to a security incident?

The answers to these questions will help you assess the level of security risk associated with a particular area of your business.

Element 1: Probability

Probability is the likelihood that a security incident will occur, independent of any effort you may make to avoid the incident. Probability is affected by factors such as your location and environment, your product, the personnel at your site, and other factors that are essentially beyond your control.

For example, if your facility is located in a high-density area of a large city, the probability of parking lot incidents and vandalism is much greater than if your facility is located in a small rural town. Or, if you use a proprietary process or have proprietary information that has a high market value, you are more likely to have theft attempts than if you don't use such a process or possess such information.

As you perform a security assessment, keep in mind that each area of your business must be evaluated in terms of the probability that security incidents will occur there. As you assess each area of your business, make a list of the most frequent incidents that have occurred in your building, at your location, and in the surrounding area or neighborhood.

Element 2: Criticality

The criticality of a security incident is the degree to which it affects your ability to do business. An incident with high criticality is one that:

- Interrupts your business operations
- Has significant operational or legal ramifications
- Impacts or reduces sales
- Erodes the quality of your products or services
- Gives the competition a significant advantage
- Causes the loss of substantial revenue
- Damages the corporation's reputation

As you assess each area of your business, make a list of the security incidents that could have a high degree of criticality.

Element 3: Vulnerability

Vulnerability is a measure of your ability to prevent a security incident. Your current security system and procedures represent the active steps you've taken to decrease your vulnerability.

Vulnerability is a dynamic concept. It changes whenever your environment, operations, personnel, business and/or systems change. Each time a substantive security-related change occurs in an area of your business, you need to reconsider your vulnerability in that area.

As you assess your business, keep track of the things that make it easier to reduce the likelihood that an incident will occur, as well as the ones that make it more difficult.

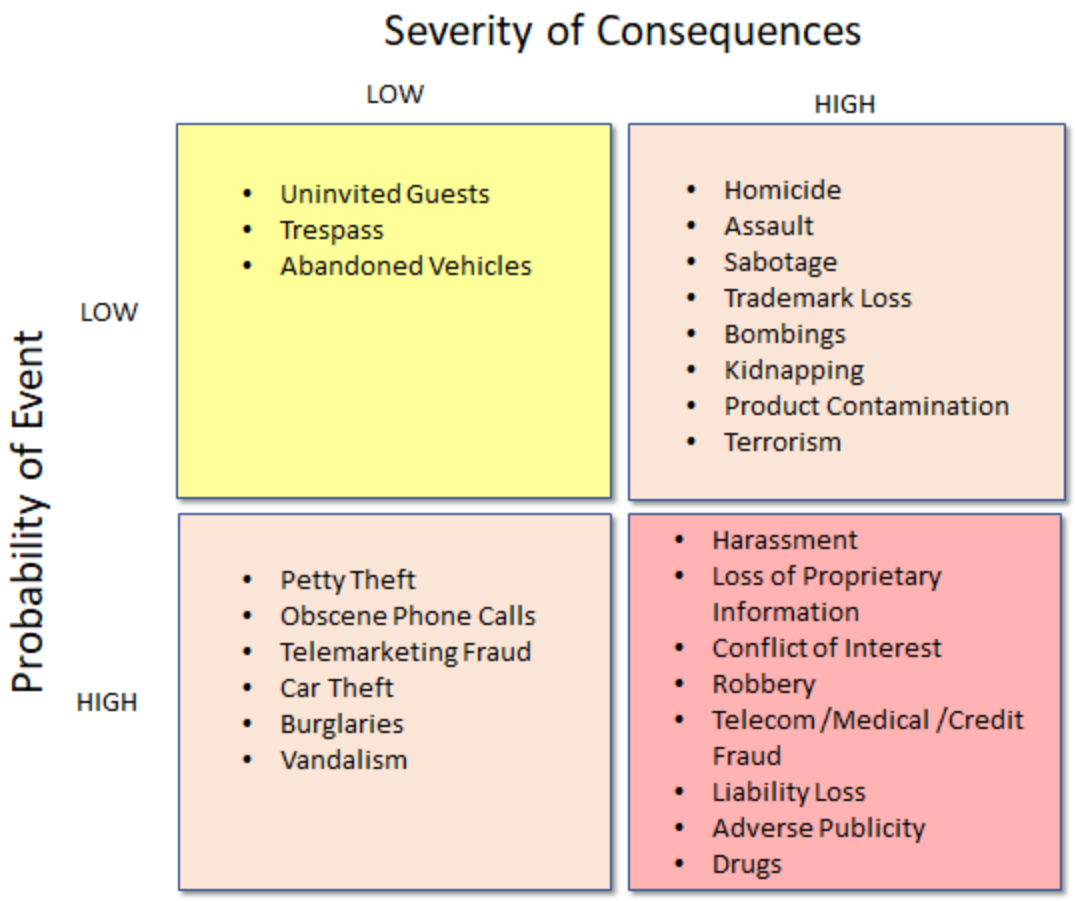
Combining the Three Elements of Security to Arrive at an Assessment of Risk
The most cost-effective security systems consider all three elements of security simultaneously to arrive at an assessment of the risk associated with a particular area. You can gauge the overall security risk for an area by determining the degree to which the area has high values for probability, criticality, and vulnerability.

It makes most sense to concentrate your resources on areas that have the greatest degree of security risk. Highest priority should be given to those areas that have high values for probability, criticality, and vulnerability.

When the values for a particular area add up to an unacceptable level of risk, it is vital that you lower one or more of them by implementing security measures. On the other hand, areas that have a uniform set of low values should not be using security resources that could be better spent in other areas of your business.

Matrix of Security Risks
Another way to look at security risks is to create a matrix of four quadrants. The quadrants are based on two High-Low dimensions: 1) the probability that a particular event will occur, and 2) the severity of the consequences should the event actually take place.

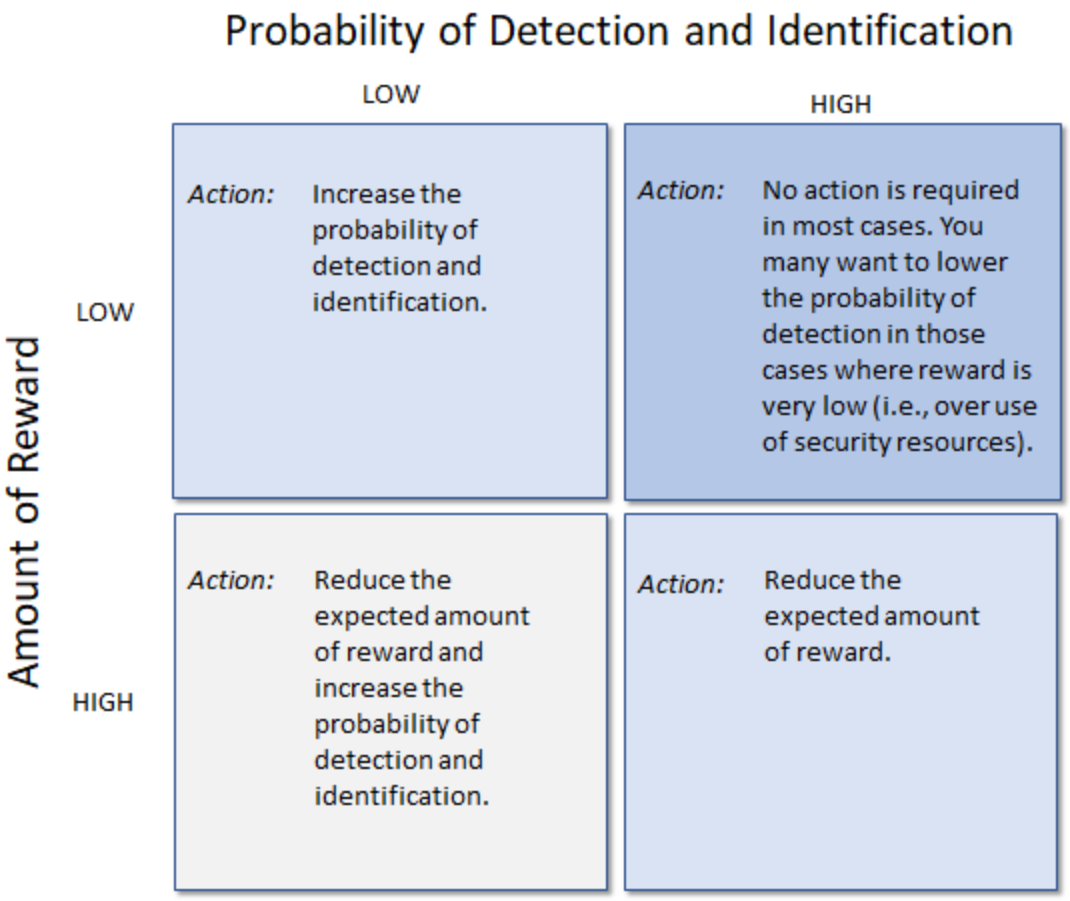
The following matrix classifies many of the events that could happen at your business by placing them in the appropriate quadrant. You may want to classify these and other events for your business by completing an exercise similar to the example below.



Deterrence: Creating an Effective Security Zone

The best security methods prevent incidents before they happen. For the most part, incidents can be avoided by creating a security zone in which individuals considering a security violation realize that the probability of being detected and identified is far greater than the reward they can expect to gain from the violation.

The following chart shows how these two factors—probability of detection and identification and expected amount of reward—interact to produce areas of effective and ineffective security zones.



The most effective security zones (shown in darker shade of blue) have a high probability of detection and identification and a low amount of expected reward. Moderately effective zones (shown in lighter shade of blue) and ineffective security zones (shown in light grey) can be enhanced by either increasing the probability of detection and identification, by lowering the amount of expected reward, or by doing both.

Visit the Security Executive Council web site to view more resources in the Program Best Practices: Policy and Guidelines series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

