The Physical Security of Police Stations and Law Enforcement Facilities

Published on February 10, 2020

Background

This article was originally published in February 2020, given recent civil unrest in large and small communities, I felt it would be beneficial to republish the article.

This weekend a shooter walked into a Police Station which resulted in the shooting and injuring of several officers. https://apnews.com/4bc2296db89a22c7c313f717ce76ff6f

Over the years I have conducted risk, threat, and vulnerability assessments of many police stations, courthouses, city halls, and other municipal structures. In those assessments, I found many of them to have significant vulnerabilities.

This issue has evolved over time, as in the past, we counted on respect for authority to minimize acts of violence. Just like courthouses, we have found that respect for authority is lacking when confronting the mentally unstable, violent offenders, and organized crime. After several courthouse attacks, the Federal Marshal's developed physical security Standards for Courthouses which has spawned State and Municipal Standards. This has resulted in much safer courthouses. The first part of implementing this Standard is a full Risk Assessment. You cannot address problems until you know what are the problems and risks. Isn't it time we applied similar standards to police stations?

Threats

Let's start with the threats, they include Domestic Violent Extremists, Homegrown Violent Extremists, Political and Civil Unrest, Disgruntled Citizens, Disgruntled Employees, and the Mentally Unstable

Known tactics include assaults with edged weapons and/or small arms, and improvised explosive devices.

Areas of Concern

Areas concern in most police organizations include;

- Access of people into the building
- Afterhours access
- Law Enforcement only access
- Duress alarms
- Response mechanisms
- Staffing during the workday and after hours.

- Interior Access
- Public Parking
- Staff Parking/Law Enforcement Vehicle Parking
- Public Counters and Offices
- Public lobbies, hallways, stairwells, and elevators
- Screening mail and packages
- Physical Security Systems (cameras, access control, visitor management)
- Plans, Policies, and Procedures

Detection, Delay, and Response as a Metric

As with any physical security system, these three items are how we evaluate performance and manage effective physical security.

Detection

Detection speaks to the ability of the system to detect an adversary action. Detection really consists of four performance measures. The first performance measure is the probability of detection. This is the probability of detecting our adversary. The time between sensor activation (notification) and assessment (human evaluation that an intrusion is occurring) is a very important metric for detection. If we have a good system, then the assessment is rapid and accurate. Conversely, if the assessment is delayed, it gives the adversary time to complete their task and leave. So, the longer the time between sensor activation and assessment, the greater the opportunity is for the adversary to be successful.

A key principle in an effective integrated physical protection system is; *detection is not complete until the alarm is assessed*.

Delay

A delay provides obstacles to slow the adversary and increase adversary task time. This can be accomplished with barriers such as fencing, cages, bollards, access control points, turnstiles, and hardened rooms in a layered design. The intent is to cause an adversary to possess many kinds of skills and tools to be successful in breaching the series of delays.

Response

The response is related to the quality of the response. The response function begins at first detection. To have a quality response the integrated system calls for the response force to respond, they deploy to the right place and nullify the adversary. The process entails two components. The first is the interruption of the adversary and the second is nullification.

The performance measures are;

- The probability of communication to the response force includes; alarm reporting to an operator for assessment and communication to the response force after assessment. It further includes the time it takes to communicate accurate information to the response force.
- The probability of deployment is the probability that the response force will be at the right place with the right number of people and with the right equipment.
- Time to deploy this is a very important factor that contributes to analytical models used in assessments. Time to deploy is important because if it takes longer to arrive at the scene and deploy than it takes for the adversary to complete their task than the adversary is successful.
- Response force effectiveness relates to the abilities of the response force and if they are superior to the adversary. In other words, if your adversary is three trained terrorists with military experience, small arms, and explosives, a single police officer is inadequate to defeat this adversary.

In summation, we want the earliest possible detection and enough delay features, to allow our response force to arrive in time to nullify the adversary.

Layered Security or Security In-Depth

Layered Security relates to “Concentric Circles of Protection” also called "Security in Depth". In this concept, we use multiple “rings” or “layers” of security where each layer is more complex and requires a different skillset and tools to breach.

The first layer is located at the boundary of the site, and additional layers are provided as you move inward through the building toward the high-value assets. The first boundary also provides us the first opportunity to detect an adversary action is taking place. Of course, this requires that technology be present which is capable of sensing and detecting the start of an event.

Basic Principles

Basic Principals of Security Layers

You can divide access into a facility into use areas for example the most exterior layer is for guests, contractors, and deliveries. The next layer is mixed-use for example meetings between employees and guests. The most interior layer is the most protected and is only accessible by qualified employees. Depending on the facility and the nature of its business there can be more than three principal layers. Having multiple layers ensures that an intruder will not be able to gain access to sensitive and controlled areas.

We can decrease the possibility of adversary success by adding layers, or by increasing the effectiveness of each layer, or by doing both.

Relying on a single physical security layer is not very effective.

When all is said and done the question is how well is your agency prepared?

It is time to start considering the vulnerabilities of our police agencies. Although many large agencies have exceptional security at their headquarters, many precincts, medium, and small agencies do not have the same level of security and protection. With a few exceptions, most police officers are not

physical security or risk specialists. It is time for these agencies to engage Certified Professionals to assist in a risk assessment, develop mitigations, and secure the facility.

In the end, we have a duty to protect our highly trained first responders, we no longer have the luxury of counting on respect for authority.

If we can assist you in conducting a risk, threat, and vulnerability assessment please reach out.

Thank you,

Jeffrey A. Slotnick, CPP, PSP

President, Setracon Inc.