



Whitepaper: Mission Critical Facility Security

WHAT'S INSIDE

Government facilities increasingly are becoming the target of hackers, cybercriminals, and active shooters. This whitepaper scratches the surface on tactics that can be employed to protect facilities, employees and data.

A Checklist for Securing Public Safety Answering Point Facilities, Personnel and Data

A Significant Threat to Emergency Communications Systems

Earlier this year, the U.S. Department of Homeland Security (DHS) issued an alert indicating that government facilities increasingly are being targeted by hackers and cybercriminals, a trend that DHS expects will increase. This includes public safety answering points (PSAP), aka 9-1-1 centers. Sometimes, personnel click on a link found on a website or in an email and unwittingly unleash a computer virus or malicious code known as malware. Often the breaches come in the form of denial-of-service or ransomware attacks. In the latter, hackers infiltrate a communications system to place malware that encrypts the agency's data, then demand a ransom to provide a decryption key.

Such an attack on a public safety agency could result in its automatic location identification (ALI), automatic vehicle location (AVL) and geographic information system (GIS) data becoming compromised or inaccessible, which would have a dire effect on emergency response. It is a significant concern.

Unfortunately, it is not the only worry. Data breaches often are self-inflicted wounds, and any number of potential circumstances can lead to a facility breach. In this whitepaper we explore a few best practices designed to keep public safety facilities, the people that work in them, and the data they work with, safer.

A Surprising Enemy

Walt Kelly's iconic cartoon character "Pogo" once famously uttered, "We have seen the enemy, and he is us." That statement certainly can be applied to the public safety sector.

Employees who work in public safety facilities generally understand the importance of rules and regulations compliance. They likely sign a form every year that states giving information to unauthorized parties could be grounds for discipline, up to and including termination. In addition, law-enforcement dispatch personnel deal regularly with their individual state's criminal justice databases, as well as the Federal Bureau of Investigation's National Crime Information Center (NCIC) databases, all of which are subject to stringent security practices.

Nevertheless, things happen, because humans tend to make mistakes or exhibit poor judgment.

For instance, the DHS conducted an interesting experiment in 2011: it dropped computer disks and USB sticks in the parking lot of some government facilities. Amazingly, 60 percent of the employees who found the devices plugged them in to their office computer—and if the device had any type of departmental logo on it, 90 percent were plugged in.

Usually, however, breaches are borne of comparatively benign circumstances. Agencies typically change passwords often, which generally is a good idea; but remembering passwords can be difficult, so employees write them down, often on sticky notes that they then attach to their computer monitors for ease of access—which also makes them easily accessible to anyone who walks past the workstation. Increasingly, agencies are allowing employees to bring their personal devices into the workplace and plug them into the network. This is problematic because all sorts of malicious code can be lurking in those devices, just waiting for an opportunity to infiltrate a network whose defenses have been circumvented. Finally, employees usually do not log off the network when they temporarily leave their workstations—perhaps to get a cup of coffee—which is ample time for someone to use their workstation to launch a cyber-attack.

Simple, yet Effective, Steps to Protect Your Networks and Systems

There are a lot of things that can go wrong concerning cybersecurity. Here are a few things you can do to protect your networks and systems:

1. Develop and, more importantly, enforce clear policies that govern the connection of personal devices to the agency's networks and systems.
2. Require employees to log off, or lock, their workstations any time they are away from them.
3. Escort visitors, even known vendors, at all times when they are in the facility, especially when they are on the public safety facility communications floor or in any of the equipment rooms.
4. Continually remind employees not to store written passwords where they easily can be discovered—especially on their computer monitors or under their keypads.

The cybersecurity threats faced by PSAPs and related public safety agencies are real and they are increasing; self-inflicted wounds such as those described above only make it easier for such attacks to occur. The best way to combat this is to invest in continual education about security issues in order to keep them top of mind with your employees, so that they fully understand the seriousness of these threats and, more importantly, realize the vital role they play in preventing them.

Enemies at the Gates

While it is the cybersecurity breach that typically receives the headlines, physical breaches of a public safety facility can be equally devastating. Sometimes such intrusions are quite innocent. For example, one 9-1-1 center had the misfortune of being located near a building that caught fire. Because the PSAP did not have a security damper system on its air-intake vents, the thick, acrid smoke could have entered the facility, and the personnel quickly would have been overcome. Fortunately, a strong wind blew the smoke away from the PSAP, averting a potential disaster.

Sometimes physical breaches are on purpose. Here's an example: a PSAP employee once was involved in a road-rage incident that concluded in the facility's parking lot. The lot was secured, but the entry gate was on a time delay; the other party who was pursuing the employee was right on his bumper, close enough so that he was able to enter the lot before the gate closed. It is not inconceivable that the altercation could have continued inside the facility itself.



Requiring employees to log off, or lock their workstation when they are away is an important, but often overlooked, step to protect your organization.

Plan for Security Before Site Construction Begins

Ultimately, facility security is the first line of defense in protecting personnel, the systems on which they work, and the data those systems generate. Here are a few best practices to follow that will enhance facility security:

Avoid site locations where accidents could occur nearby.

- Often, PSAPs are limited to land that the county or municipality owns. But those that are able to choose their locations should avoid a location that is near an interstate highway or freight rail line. Trucks and trains occasionally are involved in accidents that cause them to spill their cargoes, which can create a hazardous-materials (hazmat) incident for the facilities that are located close to the accident. And, it is not unheard of for a truck to leave the highway as the result of an accident and crash into an adjoining building. PSAPs should avoid being that building, if at all possible.
- Avoid being in a 100-year floodplain at all costs, for obvious reasons.

Allow adequate areas to accommodate security measures such as fencing, setbacks, berms and parking lots.

- When selecting a site, choose one that provides adequate area to accommodate security tactics such as perimeter fencing, setbacks, berms and separate employee and visitor parking lots.
- Regarding perimeter fencing, make sure that it is at least eight-feet high, as people have been known to drive their car up to the fence, climb onto the hood, and then leap over the fence.
- Also consider interweaving fiber-optic cable into the fence; if someone tries to scale the fence, the light-carrying properties of the cable will change, which will trigger an intrusion detection alarm.
- Ideally, the gate will be one that slides open and closed, and not the less-expensive arm that simply raises and lowers—and which easily can be crashed through.
- Creating an earthen berm is an easily executed and relatively inexpensive physical security measure. In addition to preventing vehicles from crashing into the building, it provides an effective physical barrier that prevents agency personnel and their activities from being observed. When creating a berm, make sure that it is four-to-six-feet high.

Plan for varying needs of employees and visitors for parking, building entrances, and security purposes.

- It is a good idea to have separate parking lots and entrances for employees and visitors.
- A card-access control system ideally would be utilized at the employee gate and building entrance.
- In addition, the employee entrance should have a secondary means of authentication—the gold standard would be some sort of biometric system, perhaps one that scans fingerprints or hand geometry. Retinal scanners also would work well, but they are more expensive and many people are worried about whether they are safe to use.
- Though the least-expensive option, personal identification number (PIN) pads should be avoided for this purpose. While the typical four-digit pad has 9,999 different numerical combinations, it is relatively easy through various means to determine the four digits of the current code; so, that reduces the possibilities to 16 combinations. However, the use of hardware or software “tokens” that automatically regenerate the security codes at fixed intervals is an effective workaround.
- Regarding visitors, issuing them self-expiring badges is a very effective security measure. Once the badge is peeled from its backing, a chemical reaction begins that is triggered by the badge coming into contact with oxygen; in a few hours, red “Xs” appear on the badge, preventing it from being handed off to another party if the PSAP personnel forget to collect it when the visit concludes.

Trends & best practices to enhance facility security at public safety facilities

- 1 Smart Site Selection** 
- 2 Site Security Measures** 
- 3 Employee Vs. Visitor Entrances** 
- 4 Sally Port Entrance** 
- 5 Biometric Systems** 
- 6 Card-Access Systems** 
- 7 Video Surveillance** 
- 8 Retinal Scanners** 



- Also, it is a good idea to construct the visitor entrance with a vestibule that features a “Sally Port,” the key attribute of which is a series of locking doors that will not open until the previous door closes, which will prevent someone from rushing into the building. The vestibule also should have an audiovisual intercom that allows agency personnel to screen any visitors before they are permitted to enter the facility. All visitors should be escorted, even if they are known and badged, especially if they will access the 911 floor or the facility’s equipment rooms.

Consider adding video surveillance and a security damper system as additional means of security.

- Speaking of video surveillance, it ideally would be implemented along the perimeter of the facility, and the cost of such systems have decreased dramatically over the years. However, if budget is an issue, at the very least, consider deploying a surveillance camera at the front gate and main entry door. Data analytics then can be leveraged to determine when the camera image changes, such as when a vehicle pulls up to the gate—when it does, the system will trigger an alarm.
- Finally, as suggested above, install a security damper system on the air-intake vents that can be triggered with the push of a button. Such vents typically are four to six feet above ground level, which would make it easier for a prankster—or more nefarious actor—to introduce a caustic substance into the facility’s air supply.

Conclusion

This whitepaper only scratches the surface of the tactics that can be employed to secure PSAP facilities, personnel and data. But it’s a great start—and when it comes to security, every little bit helps.

THE LEADING CAUSE FOR BREACHES

More often than not, human error is a major factor with security breaches.

Most security breaches are borne of comparatively benign circumstances, such as routine password changes or the use of personal devices in the workplace. Even underlying issues that enable many phishing, hacking and malware incidents often can be attributed to human error in some way. The numbers show that human error is a factor more than half the time.

About Mission Critical Partners

Mission Critical Partners is a professional services and network and IT support firm that helps clients enhance and evolve their public safety systems and operations through extensive experience, knowledge and resources. By providing insight and support every step of the way, our clients are able to transform their mission critical operations, maximize the value of their investments and ensure optimal performance and success.

For more information, visit MissionCriticalPartners.com

Mission Critical Partners
690 Gray's Woods Blvd.
Port Matilda, PA 16870
Phone: 888.8.MCP911 or 888.862.7911
Fax: 814.217.6807