THE SafeHarbor® BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - March 2019

DEFENSE IN DEPTH

Physical Security Part II

Our defense in depth series continues with interior physical security. Now that you have addressed the physical exterior, it is time to look at security concerns on the inside of your organization.

Organizations should not only be concerned with intrusion, but all forms of loss prevention. Loss can result from theft, fire, natural disaster, system failures, and even human error. Each organization is unique, and there is no one size fits all solution when it comes to security. We will discuss key considerations in the following sections.

Assessments

When it comes to protecting vital assets, the key to success begins with a Business Impact Assessment (BIA). By identifying things that are important and have the most value to your organization, you can identify what needs to be properly protected. It is important to emphasize here that intellectual property may be difficult to assign value to because of the cost to recreate it.

The next step is to develop a Risk Assessment (RA) for those items, so you can formulate a plan to protect them. Once you identified what is important to your organization and potential risks, a security strategy can be developed that provides a balance of protection based on cost and value. In the case of physical devices, it may be less expensive to replace them, but the time lost waiting on replacements may not be acceptable and could put your business at risk.

Alarm Systems

Typically, the first layer of interior defense is an alarm system. As discussed in the previous newsletter, budget and overall requirements will determine what type of system you acquire. Your alarm system must alert you to intrusion, fire, health, and safety threats. With such a broad spectrum of threats, it is not unusual to require multiple alarm systems to accomplish this task.

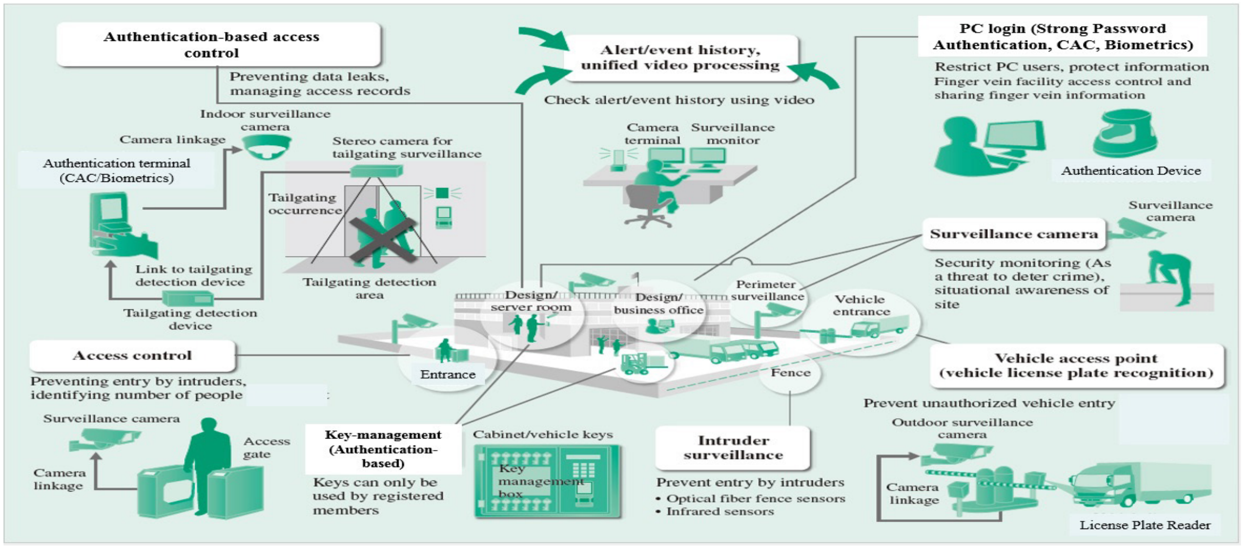
All alarm systems should be automatic and include human inputs, such as manual fire alarm stations, panic buttons, and wireless key fobs. Ideally, locations with human inputs would provide alarm monitors and first responders with a specific location.

Often an alarm fails to protect personnel and property because a response plan is not in place. Without a response plan, your organization is left to guess what to do next. Those delays can cost your organization, both in physical and monetary loss. By planning ahead, you can protect what you have and recover quickly.

Access Control

The next layer of defense is access control. Depending on your business, you may or may not have a public facing facility. However, every organization has locations that are restricted from public access, like communication closets, alarm systems, and other private locations. Based on your BIA and RA, those locations may require anything from a key and lock to biometric identification and pin to gain access.

Access control is not limited to locking devices. It also includes construction requirements, personnel identification, authorization systems and database, and training. As with the locks, the BIA


Authentication-based access control
Preventing data leaks, managing access records
Alert/event history, unified video processing
Check alert/event history using video
PC login (Strong Password Authentication, CAC, Biometrics)
Restrict PC users, protect information
Finger vein facility access control and sharing finger vein information
Authentication Device
Indoor surveillance camera
Camera linkage
Authentication terminal (CAC/Biometrics)
Stereo camera for tailgating surveillance
Tailgating occurrence
Camera terminal
Surveillance monitor
Link to tailgating detection device
Tailgating detection area
Tailgating detection device
Surveillance camera
Surveillance camera
Security monitoring (As a threat to deter crime), situational awareness of site
Design/ server room
Design/ business office
Perimeter surveillance
Vehicle entrance
Access control
Preventing entry by intruders, identifying number of people
Entrance
Fence
Vehicle access point (vehicle license plate recognition)
Prevent unauthorized vehicle entry
Surveillance camera
Access gate
Camera linkage
Key-management (Authentication-based)
Keys can only be used by registered members
Cabinet/vehicle keys
Key management box
Intruder surveillance
Prevent entry by intruders
• Optical fiber fence sensors
• Infrared sensors
Outdoor surveillance camera
Camera linkage
License Plate Reader

and RA will help determine what your organization needs. Other requirements may also be mandated by laws, industrial standards, and other directives; however, the weakest link with any access control system is normally human error.

Training

Training is a necessity to prevent human error. Every new employee should be trained in access control requirements, challenges, and reporting. This training should be continually enforced through email, posters, newsletters, or other forms of communication used by your organization. Training refreshers should be provided at least annually and any time a process or procedure is updated or changed.

Often access control training provides individuals with a set of procedures to read. Keep in mind that with this level of effort, the expectations for retention and perceived importance are low. If the cost of training is prohibitive and reading the procedures is what you must do, require a passing score on a quiz or exam to emphasize the training's importance.

Other Considerations

Climate control and lighting are often overlooked yet very important to the security and safety of your organization. Besides the obvious health and safety issues for employees, there are safety issues related to equipment as well. Electronics are very susceptible to damage from heat, humidity, and static electricity. Depending on your BIA and RA results, an investment in backup power may be required. You may only need enough power to gracefully power down equipment, which can be provided by a bank of batteries or backup generators. This also includes the decision for what equipment requires power and what is not necessary in the event of a failure. Portable air conditioning (AC) units are often used to prevent damage to server rooms in the event of climate control failure, so service is not disrupted. Even portable fans can help cool your vital electronics.

Plans

Every strong security plan includes a thought out and well-practiced evacuation plan. It is not simply the thought of getting people out and allowing emergency services in. You must protect operations as well. All your security is lost when you just open the doors. Of course, employees' safety is always a priority. With some forethought, your plan can achieve employee safety and maintain security at the same time. Your evacuation plan needs to protect your organization also by offering control of entry and egress points along with accountability.

Finally, you should have a Disaster Recovery Plan (DRP) beginning with an inventory of what was lost (facility/personnel/equipment/data) and prioritizing your recovery based on the BIA. This could be a matter of transferring operations to an alternate location, installing new or leased equipment, utilizing any variety of cloud services, or simply reloading a backup from off-site storage. Another important plan is an Incident Response Plan (IRP), which is practiced, refined, and practiced again.

Again, the key to success is having a plan, exercising the plan, and implementing lessons learned from those exercises.

Now that you have established both exterior and interior physical security for your organization, you want to know it is working. Some organizations test security boundaries themselves while others hire outside non-biased penetration testers. We recommend both, a continuous internal process along with regular outside evaluations.

About Gnostech Inc.

Gnostech Inc. is an engineering and security consulting company focused on the defense and maritime industries. We have over 35 years of experience developing products and solutions to address the technology and security needs of our customers and clients. To learn more, visit www.gnostech.com.