

THE SafeHarbor® BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - June 2019

DEFENSE IN DEPTH Controlling Facility Access

Controlling access to your facility is essential to any Information Technology (IT) system. In some cases, it is easy. You just put up a fence and lock the gate initiating a “non-shall pass” concept. This is not a viable option in most cases. You need to interface with the public to do business.

Organizations must develop a facility access strategy for increasing levels of restriction that allows public access where necessary and blocks unauthorized access to sensitive locations while providing a level of security from potential threat actors. Here are some key considerations when developing a facility access strategy.

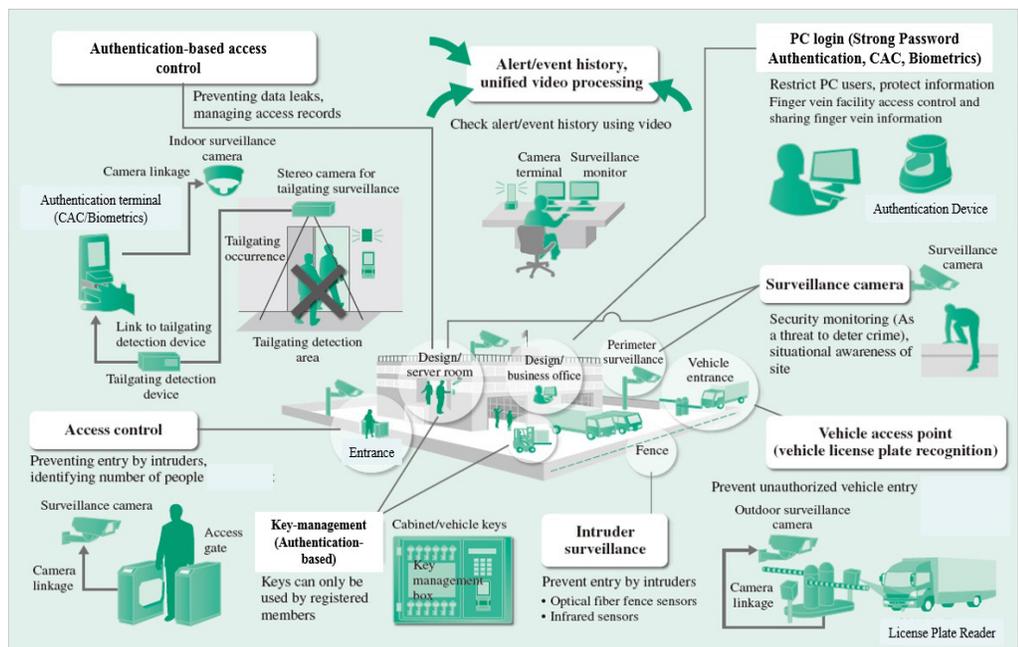
Planning and Risk Assessment

As with any worthwhile endeavor, we must start with planning and an initial risk assessment. Understanding such threats and vulnerabilities help determine what needs protection, its value, and a reasonable monetary expense to protect it. With this knowledge in hand, a reasonable plan can be developed to control the access to your facility. It is important to note that every location has different needs. If you have multiple facilities, each facility will need an individual assessment to develop an effective and tailored facility protection plan for each.

Cost

Cost is always a limiting factor when developing an access control plan. When the budget gets thin, organizations are usually quick to cut funding for security, training, and safety. However, this is not always the best plan of action and could result in major financial loss resulting from theft, error, or neglect. To quote Benjamin Franklin: “an ounce of prevention is worth a pound of cure.” With that in mind, make sensible decisions when planning based on defensible reasoning.

An appropriate level of research is required to pick the right solutions for the job. For example, lighting can be a major expense and comes in many shapes and sizes. If you purchase the wrong type of light, you could be spending money that provides too much or too little security. For reference, the Illuminating Engineering Society (IES)’s “The Lighting Handbook” is considered a staple in the compendium of lighting reference guides for the industry. The Department of Defense (DoD) initiated an excellent free resource, the Unified Facilities Criteria (UFC), that addresses Interior



Typical layers of access control



and Exterior Lighting Systems and Controls (UFC 3-530-01) and Security Engineering: Entry Control Facilities/ Access Control Points (UFC 4-022-01). Also, the National Institute of Building Sciences has a plethora of information and is another excellent resource.

Another cost savings technique is the ability to turn elements on and off when the threat levels are altered. Examples include: hiring a security guard service to patrol the facility perimeter, back-up generators, or tethered blimps/ unmanned aerial vehicles (UAVs) for an eye in the sky. Things you do not normally use but could when matters rise help preserve your security posture when events change. Why? Things can change in an instance like severe weather or demonstrations turning into a riot. Having a Plan B leaves you with options when the unexpected happens.

Security

Do not forget about the hidden costs of security. In your effort to control access, you will acquire large quantities of personal information you must protect. Every country, state, and city observe privacy differently and you must ensure you address all regulations. Cameras are a good tool for surveillance, but your neighbors may see them as an invasion of their privacy. Some high-end locations may have rules that protect the scenic view, requiring cameras and antennas to look like part of the landscape.

Another security issue your plan must address is emergency evacuation, shelter in place, or facility lock down. You want to get people out safely, emergency services in, and still protect your corporate property during an evacuation. Sheltering must provide a safe location from the threat of tornadoes to an active shooter. So, your plan must identify suitable locations to shelter and a means to communicate that it is safe to leave the shelter when the emergency event is over. An efficient lockdown may require coordination among parties to accomplish this task. Rehearsals and practice drills may also be necessary.

Larger facilities may require motorized transportation to patrol and respond to alarms. You do not need to bust the budget and purchase a four-wheel drive (4WD) all-terrain vehicle if a golf cart or Segway can meet the need. The same goes with waterways, you may need a powerboat to cover a vast area quickly or an aluminum boat with trolling motor may be enough. However, make sure your choices can handle inclement weather conditions for your area. You may need specialized equipment in this instance. Security forces on foot also need to be adequately protected from the environment.

Communication

Your plan must address communication. Here is just a sample of questions your organization should discuss:

- How will you communicate, who needs to be in the loop, what needs to be communicated and when?
- Are cell phones enough and are radios needed?
- Do you need encrypted communication to keep matters private?
- What is your backup plan if those devices fail?

You may need a public-address system or a reverse 911 capability. Communication includes alarms and panic buttons. It is vital that any of these communication methods be regularly tested to ensure performance during an actual emergency event. Planning access control for facilities is complex, with many factors that need to be taken into consideration. No organization is the same and each facility access strategy will be unique to them.

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.