THE SafeHarbor® BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - January 2019

DEFENSE IN DEPTH

Physical Security

There is an old saying, “Locks don’t keep people out, locks keep honest people honest.” This holds true with cybersecurity. Your efforts to keep people out can and will be breached. That is why you need defense in depth. No one barrier will stop a breach, but multiple barriers decrease the likelihood of intruders going unnoticed.

Defense in depth is often described as the “onion skin” approach by implementing layers of security within your network design. Our new series of newsletters will address these layers of security, and we will start from the outside with physical security.

Physical security includes everything you put between the public and physical access to your Information Technology (IT) infrastructure. The military calls it “Gates, Guns, and Dogs” for short, but it is more than just using guards. There also needs to be a balance between security and ease of customer access.

Determine Physical Security Threats

The first step is to determine what threats exist for your location. For example, if you have a concern with terrorist bombings you need separation or barriers between your building(s) and roadways, parking, and vacant neighbor buildings. You also need to have a clean open area outside the building so anything maliciously left beside your facility can be easily observed. This separation reduces the effectiveness of explosive devices. If you do not have a fence around your outside border, consider using trees and large stones to keep motor vehicles out.

Ports are full of people and vehicle traffic. Clear signage indicating traffic patterns, highlighting exclusive zones will help security identify a person or vehicle who is in an unauthorized part of the port and could pose a threat.

As a rule, physical security is not about preventing someone access but making it difficult and increasing the likelihood of being caught. When you purchase a safe or locking container they come with a rating for fire and access. Underwriters Laboratories (UL) use a “TL” rating to determine how long it takes to access the container using standard tools.

External Access Points

Criminals gauge risk of getting caught by the time it takes to gain access. So, choosing your building materials is key to increasing that difficulty. A common home wood frame door is easily accessed with a little muscle and a crowbar, but a commercial steel frame door requires a lot more effort to force open. Along with the door construction, the choice of locks adds to the time required to force entry. A trained locksmith can pick a key lock in a few seconds, but a combination lock requires tools and several minutes to gain access. Electric strike plates tied to biometric or card readers allow easy access with stronger security.

Safe Classes	
Class 1	Any fire-resistive safe or steel container with a container lock.
Class 2	Designed for low commercial cash risk, including ATMS.
	Minimum requirement of 1-inch steel body and 1.5 inch steel door with combination lock.
	A light weight container, that is normally reinforced or encased in concrete or welded to a steel structure.
	A UL rated TL-15 would be eligible.
Class 3	Burglar-resistant safe suitable for average cash risk.
	Provides limited to moderate degree of protection with TL-30 and TRTL-15 rating.
DR = Drill TL=Tool TR=Torch TX=Torch and Explosives	

Examples of safe classes.

Assuming your doors afford too great a risk, criminals will look to windows or hidden access points like alleyways and roof tops. Even though breaking glass can alert others to an intrusion, it mostly won't deter the criminal element. Bars provide additional security and time to gain access but are costly and detract from a buildings curb appeal. Often the affordable and easy solution is adding alarms to the windows and any external access points.

Alarm Systems

When it comes to alarm systems, you need to decide if you want a silent alarm or full-blown horns and sirens. Both have their place depending on your needs. As a rule, horns and sirens are a deterrent in themselves directing public attention to an intruder. However, in a remote location or late at night a silent alarm leaves law enforcement an opportunity to catch criminals in the act.

Another decision point is having full time in-house alarm monitoring or using an alarm service provider. An internal alarm monitoring service normally means you have employees on site ready to respond and monitor alarm status. This requires a large investment of people and equipment and is usually limited to larger organizations with the capital to make such an investment. However, this method is also vulnerable to the insider threat. More realistic for most is an alarm service who reports alarms to your security staff and local law enforcement for a small monthly service fee.

Another underutilized deterrent is lighting. Criminals like to hide in the shadows out of sight of the public eye. A well-lighted parking lot protects your employees and the building's exterior. Also, lack of light in a location normally well lighted can draw unwanted attention for intruders trying to go undetected.

Video Surveillance

Today, video surveillance equipment is relatively inexpensive. Systems today allow for multiple cameras with large capacity storage devices. Remote notification is even readily available to your cellular phone. From doorbell cameras to night vision exterior wireless cameras, every entrance to your buildings can be viewed and recorded at a reasonable cost. Another benefit of video surveillance is being integrated in some alarm systems and detecting light color changes as movement. Cameras can come in many types including night vision and infrared, so darkness no longer provides sanctuary to intruders. They are also not affected by heat stress and cold temperatures. However, fog and inclement weather can affect camera views leaving lenses covered in moisture, ice and snow. Higher quality equipment can address these issues, but they come with a hefty price tag. It may be more economical to add some of these cameras at key locations rather than all of them.

Intruders will pick at your defenses just like a hacker will, hoping to breach each layer. For this reason, it is wise to consider symbiotic relationships within your security layers so a breach on one won't impact the others. The other option is to constant leave evolve by introducing new lines of defense or challenges. Consider a roving guard walking by the front entrance every 15 minutes on the dot. If you rotate the individual patrolling, the frequency changes and a plan to evade that 15-minute window will now fail. Finally, don't throw all your eggs in one basket. If you embrace many layers of security but monitor them all from one place, device, or system, you have created the single point of failure that will allow physical access to your facility.

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.