Creating a Cybersecure Physical Security Enterprise

Simplicity and convenience are the enemies of security

By Paul Galburt
IPVideo Corporation

This article is intended for executive and management personnel who may not have the technical expertise to fully evaluate physical security system installations, but who are nevertheless responsible for the installation and performance of these systems.

All organizations that have any kind of physical facility must be concerned with risk. Risks include incidents such as fire or flood, as well as deliberate attacks that involve theft. These risks can cause loss of intellectual property, interruption of business, or physical harm or death to members of the organization or the public.

The existence of these risks causes organizations to install and operate several kinds of physical security systems, including burglar/intrusion alarms, fire alarms, access control systems, video management systems, and overarching command-and-control facilities. While all of these systems can be effective at mitigating the above-mentioned risks, they

also represent additional points of vulnerability that must be hardened if the net effect is to be an improvement in security.

Each system's manufacturer generally provides detailed information regarding setup and configuration, but this material does not always address how to reduce the vulnerability of the very systems involved. This article offers a set of guidelines that highlight common weaknesses in the installation of these systems and explain how to reduce them.

Some vulnerabilities are the inevitable result of the addition of any complex system to an organization. (A weapon carried by a police officer who is sworn to protect and serve can be used against him, for example.) Many vulnerabilities are caused or exacerbated by the all too human desires for simplicity and convenience. (An officer might carry his weapon in a holster without a bothersome retention device like a snap, significantly increasing the risk of loss.) In order for security systems to do their jobs, additional vulnerabilities caused by these desires and resulting behaviors must be avoided. A few simple formulas may help to remind the reader of these principles:

- Simplicity = Risk
- Convenience = Risk
- Efficiency = Risk

Applying these formulas to the architecture and configuration of all of the physical security systems mentioned above will go a long way toward developing policies that reduce risk.

Passwords

Passwords are key to controlling access to all parts of a security system. But while they are extremely important, they are also very annoying. Passwords apply to four areas of enterprise operations: facility access, like door keypads; system access, like a guard's use of cameras; administrative access, for functions of management and configuration; and internal component security, such as protection of network cameras from direct access.

Facility Access

Passwords (often called PINs) for facility access are generally in daily use by every individual in an organization, so they are considered routine, and seldom is much thought given during their application.

In some cases, these passwords are embedded in a technical device, like a magnetic or RFID card. This transfers the problem to physically maintaining possession of the card. In other cases, the

password or PIN is directly employed by its owner. In this second case, simplicity and convenience come into play. A simple two or three-digit PIN is easy to remember but can be circumvented by a brute force attack. A more complex four, five, or six-digit PIN is much more secure, but is also much more likely to be written down, resulting in a discovery risk. Passwords and PINs provided to users at random are more secure than those created by the users for themselves, since the latter are very likely to be based on birthdays or other publicly available information.

Passwords and PINs provided to users at random are more secure than those created by the users for themselves, since the latter are very likely to be based on birthdays or other publicly available information.

It is convenient to keep facility access passwords indefinitely once personnel have committed them to memory, but the concurrent risk increases over time as another person may observe and make note of these passwords. Eventually, the risk of compromise rises to 100 percent. It is much less risky, though also less convenient, to enforce a policy of changing passwords or PINs on a regular basis.

System Access

Some components of a security system, such as a video management system (VMS), are intended for regular active use by security personnel. Video viewing and recording is an invasive technology, and access to such systems is usually restricted to a group of responsible individuals within an organization. These individuals generally are provided with access credentials that include a (public) username or ID and a (private) password. Simplicity suggests that such passwords not be very complex, while convenience suggests that each individual's credentials be chosen by them, that they have access to the entire system, and that their credentials remain unchanged over time. All of these policy choices, however, increase risk.

Public IDs are generally simplified and compacted versions of a user's full name, such as "jpublic" for John Q. Public, that are assigned by management. This policy allows efficient and error-free entry while allowing management to avoid duplication of public IDs. While this policy does not directly affect security, it does make entry of credentials faster and less error-prone. In some cases, a public badge number may be used as the public ID.

System access passwords are sometimes implemented as biometrics, such as fingerprint readers, but they are generally a group of letters, numbers

and special characters entered on a keyboard. All of the comments concerning facility access PINs apply here as well, with the addition of the option of uppercase and lowercase letters and special characters to the numbers that are used in PINs. While this allows for much more complex passwords, it also means that "self-chosen" passwords will tend toward the simplicity of memorable and recognizable things, like pet names, birthdates and birthplaces. These must be avoided.

Many systems allow the enforcing of password complexity policies that include requiring a chosen mixture of uppercase and lowercase letters, numbers and special characters. Although these rules are often seen as inconvenient, their use decreases risk. This is a double-edged sword as sufficient complexity often leads users to write their passwords down. A strategy or policy is required for this, too.

Systems can also enforce a password timeout in which, at suitable intervals, users are notified that they must either choose a new password of sufficient complexity or they are provided with a new one. This reduces the risks incurred by the inadvertent exposure of passwords.

In many cases, the system's resources, such as cameras, can be segregated into groups or regions to facilitate access restrictions. This may be seen as a loss of convenience, but it reduces both the risk and invasiveness of the system without loss of operational efficacy.

The organization's human resources department or its equivalent must be empowered to immediately remove the credentials of any employee who is discharged for any reason. While this is true for all employees, it is particularly germane to those with access to security systems, and is directly focused on those who might install some kind of backdoor account that is hard to detect.

> While implementing limited permissions may be time consuming and inconvenient, the practice is essential for good security.

Most systems are provided with several standard default accounts for convenient initial setup. While leaving these in place is a common practice, it is a serious security breach. Such accounts must immediately be removed or have their passwords changed to secure formats and not widely distributed. No matter how obscure such accounts are, they are well known to installers and thus effectively available to anyone.

Many systems permit adding limitations to the permissions granted to each access account. For example, security guards may be allowed to view cameras and archives, but not be permitted to export footage that might subsequently appear on

Facebook. While implementing limited permissions may be time consuming and inconvenient, the practice is essential for good security. The effort required can often be reduced by placing users in groups defined within the system and assigning permissions to the group as a whole.

System access accounts are generally denied permission to make configuration changes to the system, this function typically being reserved for administrator-level personnel.

Administrative Access

People with administrative access accounts are frequently termed administrators or admins. These accounts allow access to settings that can overtly or surreptitiously destroy the efficacy of the entire system. Since this can be done accidentally or maliciously, administrative personnel must be carefully vetted in all respects.

These accounts are also subject to all of the policies of system access accounts noted above, except that the scope of their permissions is generally enterprise-wide rather than being restricted to regions.

Simplicity and convenience must especially be eschewed here, with the accounts given high-complexity passwords with definite timeout policies.

Internal Component Security

Physical security systems generally comprise multiple components connected by data networks such as Ethernet. These components, including cameras, door locks, badge readers, alarm panels, computer servers, workstations, etc., must communicate with each other in order for the system to operate as designed. Unfortunately, every communication path (primarily on the data network) is a potential entry point for anyone with a nefarious interest in the system. The servers are the most susceptible components, having access to all of the software and everything else, but every component has vulnerabilities.

Physical Access

Computer servers are often installed in any convenient location. This is a security risk. All servers and network switches should be installed in physically secure locations where only administrative personnel can gain physical access to them without alarms being raised. Using cameras, alarms and access control equipment on and around the server room doors are reasonable precautions.

Uninterruptible power supplies (UPSs) should be located within the same secure spaces as the servers

and network switches. This prevents attackers from sabotaging the entire system simply by cutting the server power supply.

Network cables must run throughout the enterprise facility, but housing them in metallic conduit wherever possible is a good precaution to take.

Other components must be installed in generally accessible spaces, but implementing measures such as high-ceiling mounting locations and tamper-proof screws helps to mitigate the risks.

Computer servers are often installed in any convenient location. This is a security risk.

Credentials

Each component that is connected to the network generally has credentials (ID and password) that protect it from direct access. These credentials are used by the servers to make secure connections but are not otherwise used by human operators under any normal circumstances.

These components are most often delivered with default credentials in place to facilitate installation. Unfortunately, many installers leave these credentials in place for convenience or to simplify their jobs by using the default credentials in the final system operation. Nobody sees these credentials on a regular basis, so this egregious security breach is out of sight and out of mind.

Any system security audit must ascertain that these internal credentials have been changed to include high-complexity passwords that are different for at least each class of device. These passwords are not likely to be changed frequently, if ever, so the list must be kept under a highly secure master password and/or on a paper in a physically secure location.

All servers that require access should have secondary administrative accounts installed that can quickly be deleted if changes occur in the personnel who have access to them.

The data that travels between devices can sometimes be encrypted. The requirement, feasibility, added effort, and cost of this extra step should be discussed with the system engineers and installers.

Network Design

A full discussion of network design and how to optimize network security is beyond the scope of this article, but several topics form a useful start in understanding the related issues.

The overall network architecture is often designed by systems integrators, either independently or working with an organization's IT personnel, and many decisions are driven by factors other than security considerations. However, several areas are amenable to increased security, albeit at the expense of some convenience.

Network Ports

Each network-attached component, such as a camera, door controller or alarm panel, communicates using one or more network port numbers that were designated during the configuration of the system. Manufacturers always provide default port numbers and using these is the simplest way for the installer to configure the system. But good security is built in layers, and the extra work of changing the network port of every network-attached component to something different from the manufacturer's default value adds another layer of protection against anyone attempting to gain illegal control of a network device.

Private Networks

Networks within a physical location or building are generally open and unencrypted. Any network that extends through public and unmonitored space, and particularly over the public Internet, though, must be effectively secured. This security is often provided by use of a virtual private network (VPN). A VPN is really just a software protocol that includes a powerful encryption service so that the network data, even if intercepted, cannot be read or understood without great difficulty. The data is decrypted at the receiving end of the VPN.

VPN encryption and decryption services are provided by either dedicated hardware devices or software running on a computer workstation.

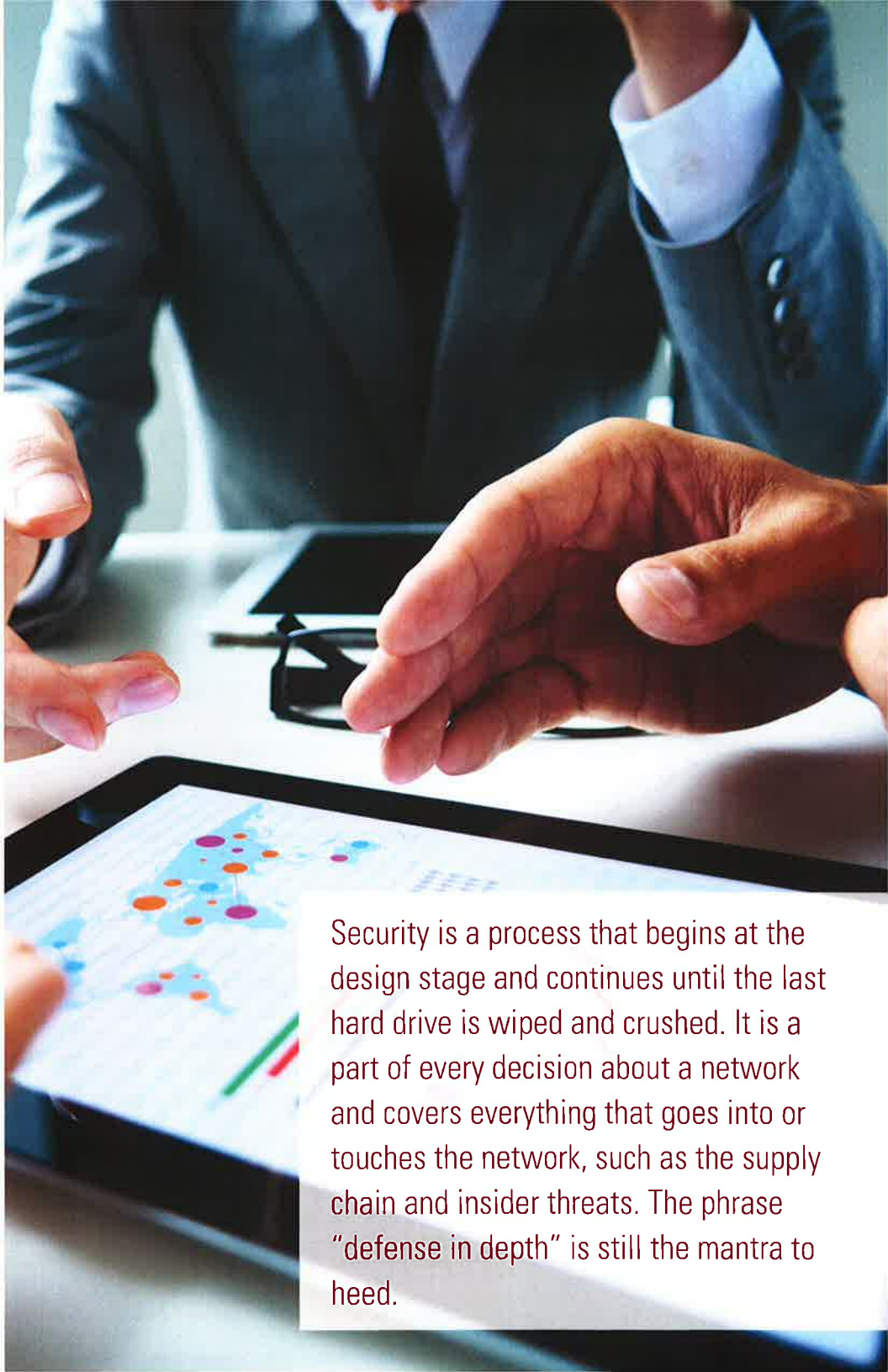
Summary

By now, the reader should have gained some understanding of several relatively non-technical, but still very important, factors that affect system security, and of the tradeoffs that must be made as part of the installation plan. These tradeoffs should be carefully examined and reviewed with the original formulas in mind:

- Simplicity = Risk
- Convenience = Risk
- Efficiency = Risk

This article has, by no means, covered every security system consideration, but the overview of the kinds of issues that are involved should enable the reader to begin to make well informed decisions about basic implementation policies, and can serve as a basic checklist for a system audit or review. ■

Paul Galburt (pgalburt@ipvideocorp.com) is vice president, advanced development, at IPVideo Corporation (www.ipvideocorp.com).



Security is a process that begins at the design stage and continues until the last hard drive is wiped and crushed. It is a part of every decision about a network and covers everything that goes into or touches the network, such as the supply chain and insider threats. The phrase "defense in depth" is still the mantra to heed.