Making Everything Easier!™

HID Global Special Edition

Advanced Physical Access Control

FOR DUMMIES®

Learn:

- **Best practices for physical security**
- **About modern security technologies and how to apply them**
- **How to use a layered security approach**

Brought to you by

HID®

Peter H. Gregory, CISA, CRISC, CISSP, DRCE

About HID Global

HID Global is the trusted source for secure identity solutions for millions of customers around the world. Recognized for robust quality, innovative designs, and industry leadership, HID Global is the supplier of choice for OEMs, system integrators, and application developers serving a variety of markets. These markets include physical and logical access control, including strong authentication and credential management; card printing and personalization; highly secure government ID; and identification technologies used in animal ID and industry and logistics applications. The company's primary brands include HID®, ActivIdentity™, FARGO®, and LaserCard®. HID Global is an ASSA ABLOY Group brand. For more information, visit www.hidglobal.com.

Advanced Physical Access Control

FOR

DUMMIES®

HID GLOBAL SPECIAL EDITION

by Peter H. Gregory, CISA, CRISC, CISSP, DRCE

John Wiley & Sons, Inc.

Advanced Physical Access Control For Dummies®, HID Global Special Edition

Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

ISBN: 978-1-118-12847-3

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Senior Project Editor: Zoë Wykes

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Custom Publishing Project Specialist: Michael Sullivan

Senior Project Coordinator: Kristie Rees

Layout and Graphics: Carrie A. Cesavice, Laura Westhuis

Proofreader: Laura Albert

Introduction

The security landscape has changed considerably in recent years. New laws and regulations have been passed. Lawsuits and liability assessments abound. Bad guys have gotten a lot more aggressive, inventive, and prevalent. It seems everyone and everything is a threat — from disgruntled workers to passers-by.

The security industry has changed to keep up with the evolving threats. Technologies have matured, emerged, and converged. Best practices have solidified, and new disciplines have been developed. But many end-user organizations have not kept up. Many are operating what were considered best-in-class systems a few years ago that are now inadequate. Many organizations are even worse off.

In this book, you find out all about the best practices in physical access control and the best ways for maximizing your physical access control investment.

How This Book Is Organized

The main purpose of this book is to acquaint you with advanced technologies and practices in physical access control systems, including the components of these systems.

Chapter 1: Using a Layered Security Approach, discusses the technologies that make up a best-in-class physical access control system and how to apply these technologies.

Chapter 2: Best Practices for Managing a Physical Access Control System, discusses the various management tasks that most smart organizations follow when operating physical access control systems.

Chapter 3: Ten (Or More) Best Practices for a Layered Approach to Security, lists 14 habits employed by organizations to bring out the best in physical access control systems.

Icons Used in This Book

Icons are used throughout this book to call attention to material worth noting in a special way. Here is a list of the icons along with a description of what each means.

Some points bear repeating, and others bear remembering. When you see this icon, take special note of what you're about to read.

This icon indicates technical information that is probably most interesting to techies and system designers.

If you see a Tip icon, pay attention — you're about to find out how to save some time and aggravation.

Chapter 1

Using a Layered Security Approach

In This Chapter

- Understanding defense in depth
- Deciphering the use of encryption keys in smart cards
- Choosing the best card and reader technologies
- Protecting the system from tampering and intrusion

A layered security approach is a time-honored technique that helps to slow down anyone who is trying to break in to a protected facility. Each layer represents another obstacle that increases the time and the effort required to break in. Multiple layers also give you additional opportunities to detect an attack.

In this chapter, I discuss some of the layered security controls that improve security and help to keep unauthorized people out.

Using Multi-factor Authentication

A single factor of identity might be sufficient for high-volume, lower-security areas. For example, you may

want to allow users to access the parking garage with just an access control card or to access the training room with only a common PIN code.

Multi-factor authentication controls should be considered for work areas containing valuable assets or sensitive information. Some examples include

- **Two-factor authentication.** This consists of combining two identity verification methods, such as something a person has (for example, an access control card) with something the person knows (such as a PIN code).
- **Three-factor authentication.** This might add a biometric (something a person is) to the equation. That would foil the crook that stole an access card and forced an employee to reveal their PIN.
- **Two-man authentication.** Also known as *escort,* this requires two separate users to get into a secure area. No one may enter alone.

Security professionals use the term "defense in depth" to describe any case in which two or more controls are used to provide redundant protection of an asset. If any one of the controls fails, the asset is still protected because the other controls continue to protect it.

For additional assurance, a trusted "digital certificate" may be installed into a smart card or USB flash memory token. Then, before granting access, the system can do a real-time check of the certificate's validity (a "cert check") using a technology called Public Key Infrastructure (PKI).

Checking digital certificates

A *certificate check process* is similar to a driver's license check that a police officer performs at a traffic stop. The officer requests the license from the driver and then runs a computer check to see whether it's been revoked. Just because the license was legitimately issued, hasn't been tampered with, and hasn't expired, doesn't mean that a judge didn't revoke the subject's driver's license privileges just yesterday. A real-time check via Public Key Infrastructure (PKI) of the digital certificate on an employee's smart card might reveal that the employer or another trusted party has recently deemed that person a security risk.

If an organization integrates its physical access control system (PACS) and a logical access control system (LACS), then you can use another factor of authentication called *location correlation*. For example, if Adam is working off site remotely logged into the corporate network system via VPN, then why did he just use his card at the warehouse door? Access denied!

Using Smart Cards versus Other Card Types

Magnetic stripe (magstripe) cards are an inexpensive choice to use for access control, but they typically employ little or no security features to protect the

card's data. The magstripe card's data can easily be read and then copied to another card (cloned). Because of this, magstripe cards are not recommended for security applications. Magstripe cards and barcodes are okay for checking out books at a library, but they are not part of a modern, effective security system.

Prox cards

Proximity (prox) cards were invented in the 1980s. A prox card contains a computer chip (more specifically, a transponder), but not a very advanced one. When the card is placed near a reader, it receives radio frequency (RF) energy from the reader, and its processor powers up and transmits its card number to the reader — and to any other devices listening within the proximity. In this book, when I refer to "prox," I am always referring to the cards and readers that communicate using low frequency (LF) 125 kHz radio waves.

In many parts of the world, prox is the most prevalent type of card and reader technology installed in buildings today. Prox continues to be installed today not only because it's easy to use, but also because many security professionals are more comfortable with prox products than some of the more advanced technologies, such as smart cards.

However, prox cards do have some limitations worth mentioning here. For example, prox transmits at a lower, limiting frequency range and lacks the additional security features of more advanced card technologies — such as two-way communication, memory space, and the processing power to handle other applications. Also, prox data is transmitted "in the clear," which is an unencrypted format that could make it more susceptible to modern day attacks, such as sniffing and card cloning.

When choosing a card technology, ask yourself these questions: Are you in a high-risk industry? Is there any reason a criminal would target your facility? Are there regulations or standards that compel you to have a stronger security system? If your answer to these is yes, then you may want to consider a more advanced technology. Read on.

Contact smart cards

A *contact smart card* contains an embedded microprocessor chip, which communicates through a grid of gold contacts on the card's surface. Contact cards are most often used for "logical access" or cyber security functions such as secure computer log-on, data encryption, or document signing, where PKI is involved.

Contact smart card readers are available for door access use. Some customers prefer the data transmission to occur over a contact interface rather than over the air. Others steer away from contact readers because the readers require users to insert their cards, causing wear and tear. The card slots are also sometimes targets of vandalism (gum, and so on) and are very susceptible to the effects of weather, such as ice and rain.

Contactless smart cards

A *contactless smart card* is essentially a miniature computer on a card. It has a microprocessor, memory, software programs (apps), security, and more. About the only key thing an office computer has that a smart card doesn't have is a power source. Like older prox cards, a smart card gets its power from the electromagnetic radio waves emanating from the reader.

Advantages of smart cards

Contactless smart cards are superior to traditional prox cards in several other ways. For starters, smart cards have

- A faster, more-capable processor
- More memory
- Rewriteable and lockable memory
- The ability to store and run software applications like cashless payment or secure computer log-on
- The capacity to hold applications that require large amounts of data, such as biometric data that facilitate the use of other security layers

With all these advantages and more, you'd think smart cards would cost more than prox cards, but typically contactless smart cards and prox cards cost about the same!

The most important advantage of smart cards is security; smart cards are far more secure than prox cards because they are built in ways that make it more difficult to extract a card's secret data. In addition, their over-the-air (OTA) data communications is more secure, as encryption is used.

Using Mutual Authentication

Mutual authentication is the process whereby the smart card and reader establish two-way trust by authenticating each other. It's more than an initial handshake, where two devices identify themselves to each other. Here's what

happens. Essentially, the reader says, "I know you're a smart card and you want to send me data so you can access this door. But, before I accept your data and pass it upstream to the access control panel, you need to prove to me you're a trustworthy card." And the card says, "Well, I'm not giving you any data until you prove to me that you're a trustworthy reader!"

The card and reader each use high-security cryptographic techniques to prove to the other that it is trustworthy. Only then does the card transmit data of consequence to the reader. And even then, the communications data from the reader to the card and from the card to the reader is encrypted using secure cryptographic algorithms.

Smart cards and readers establish mutual trust by using "*symmetric encryption,*" a form of cryptography, to prove that each knows the "shared secret." The devices also use cryptographic techniques to enable them to send encrypted data to one another. It's kind of like a meeting between two spies who establish trust with a secret phrase. The first spy says to the second spy, "The rain in Spain falls mainly on the plains." The second spy responds with "The Yankees are going to win the World Series."

Being Wary of CSN readers

Do not be lulled into a false sense of security by using smart card readers that simply read the card serial number (CSN) and then pass that data on to the access control panel for a go/no-go access decision. Using the CSN to verify the cardholder's identity is no more secure than

prox cards, and it's nowhere near as secure as smart cards and readers using encryption and mutual authentication.

CSN readers are useful in one situation: as a temporary solution to migrate from one smart card type to another. Using CSN, a single reader can be used to read both the existing cards (CSN only) and replacement cards (using the smart card security). This provides a window of time — the shorter the better — to replace older cards. When all of the existing cards have been replaced, the reader can then be instructed to turn off its CSN reading capability.

Using Custom Card Number Formats

Ordering cards with custom card numbering and a longer card format (for example, a 35-bit number instead of the standard 26-bit) adds another layer of security.

Cards with proprietary formats are typically more difficult to fraudulently obtain as compared to the industry-standard 26-bit *Wiegand* format. Proprietary cards may also provide provisions for nonduplication of card numbers. Some manufacturers' readers can even be set to ignore cards not completely conforming to the proper format, which also slows down the bad guys.

Be sure to verify that access control hardware and software being used or proposed for use can manage custom or nonstandard card formats.

Working with Unique Encryption Keys

Some security vendors use a single encryption key for all their customers. It's better to select a security vendor that is able to issue a unique encryption key for each customer.

With unique encryption keys, cards and readers for a particular customer are securely programmed with a matching encryption key pair not used by other organizations. In use, only matching cards and readers will work together, foiling attackers on several levels including attempts to use impostor readers or cards. No key from any of the manufacturer's other customers could ever be used to access your facility.

Choosing Cards Containing Diversified Keys

You want to avoid a manufacturer that stores the same encryption key in all of its cards; an extraction of the key from a single card might compromise all the cards in use in an organization. Instead, choose a manufacturer that uses diversified keys, which means that each card uses a different encryption key that is cryptographically derived from a master key. Ideally, this diversification methodology would use a public-scrutinized algorithm such as DES or AES.

Being Able to Roll the Keys

Choose a manufacturer that offers its customers the ability to "roll," or change, the encryption keys that are stored in the readers and cards. Be prepared to act quickly in case a key compromise does occur, and know how to use the manufacturer's procedures. Some manufacturers have the capability to move cryptographic data, such as keys and reader firmware upgrades, from a secure "vault" on their premises directly into the secure element inside the reader by using end-to-end security among trusted devices.

Look for vendors that can offer an additional layer of security for identity credentials. Specifically, the most innovative solutions provide a secure, standards-based, technology-independent identity data structure that wraps an additional layer of encryption and functionality around the card's contents.

Utilizing Exit Readers

If it is important to know who is in the building at any given time, a physical access control system can help through the use of exit readers. With this type of system, employees "badge in" and they also "badge out." This way the system can track or limit who is in the building at any given moment. Exit readers also provide the ability to use important security features such as tailgating prevention (see Chapter 2) and anti-passback (see Chapter 3).

Protecting the Wiring

An intruder who can access the security system's wiring may be able to intercept communications and be able to pull off a "replay," "denial of service," or other attack on the security system. An intruder may even be able to unlock doors by sending actuator "unlock" commands through the wiring.

Even with security protocols in use, the cabling that connects all components of an access control system should be protected in conduit or raceways that are difficult for intruders to access. Even if the entire wire run is not fully enclosed in conduit, using conduit in the most vulnerable publicly accessible areas is desirable. It is particularly important to protect the wiring of readers outside the building.

Protecting the Card Readers

Protecting card readers is a little more challenging, since they are necessarily exposed for use. Still, it is possible to take several measures to protect system tampering via the card readers:

- **Tamper-resistant screws, or "security screws."** Help to prevent someone from removing or disassembling the card reader, or at least slows them down.
- **Soldered, wrapped, or potted wiring connections.** Help to prevent someone from easily disconnecting the card reader from its wired connections.

- **Tamper-detection sensor.** A mechanism (switch, optical, or equivalent) that sends an alarm signal if the card reader is being tampered with (for example, the cover is removed).

Use card readers that protect their secrets, including firmware and security keys. If offered a choice, use readers that protect their keys from easy extraction. Choose a reader manufacturer that uses a secure element, such as a Trusted Platform Module (TPM), Secure Access Module (SAM), or other equivalent device to store cryptographic keys.

Protecting the Cards

Like keys, access control cards must be protected. Some of the safeguards I recommend include these:

- **Card stock.** Lock up extra card stock in a safe. Don't leave card stock in the badge printer.
- **Spare cards.** Enroll cards in the access control system only when issuing them; don't keep spare activated cards on hand, except for the smallest number of "forgotten card" spares.
- **RF (radio frequency) shields.** To prevent "bump and clone" attacks, employees can store their cards in a sleeve or badge holder that prevents unintentional data transmission. This is most effective for contactless smart cards; prox cards are not easily protected using shields.

- **Visible identifying information.** No information about the name or location of the organization should appear on the card. This might give anyone who found a lost card the location where the card could be used. Personnel should be instructed to conceal and safeguard their key cards when they are away from the facility.

Restricting Network Access to System Components

In addition to physical protection, it's vital to make sure that only authorized personnel have network access to physical security controllers and related systems.

Some of the measures to take include

- Individual logins for each authorized person
- Varied access privileges (for example, a lower-level security guard should not have privileges to enter or edit user records, or to reconfigure any system elements)
- Complex passwords that expire every 90 days or more often
- Encrypted communications only
- Firewall protection
- Network intrusion detection
- Anti-virus protection

16

Protecting the Power

Physical security systems need to have a continuous supply of electric power, even when utility power fails. A part of a system's design should include facilities to provide reliable electric power.

If the building where physical security controllers and related systems are located includes a computer room protected with an uninterruptible power supply (UPS) and/or an emergency generator, then you may want the physical security system and its components tied into those systems.

Different brands of security systems handle power outages differently, some not very elegantly or securely. I suggest you check on the specifics for any brands in use or under consideration and test it after installation.

Chapter 2

Best Practices for Managing a Physical Access Control System

In This Chapter

- Managing user access
- Making changes to the system
- Understanding system monitoring
- Educating employees
- Conducting periodic reviews

There are two vital components in every organization that does physical access management correctly: the process and the technology. In Chapter 1, I discuss technology; in this chapter, I talk about the process.

An effective and secure physical security system is only as good as the processes used to manage it. If the processes are not well designed, then the system can be like Swiss cheese: full of holes.

Access Management

Most organizations find it best to implement some form of role-based access control. As an example, while you may want to allow your warehouse worker to access the cafeteria and mailroom areas, there is probably no reason to give that person access to the finance, legal, and records storage areas. Thus, you'll need to map out access zones and time periods that allow you to control who goes where and when. And you'll likely want to assign your employees to certain groups and then give certain groups certain access privileges. Once you think you're done with that exercise, you'll be keenly aware that a lot of changes are inevitable over time. And that means you're in need of "change management," discussed later in this chapter.

It is important to have a formal, written process, including written (or electronic) records, in any user access management system. This process should have

- Formal request, review, approval, and completion steps
- Recordkeeping that tracks who is making each request, for whose access, for what zones, and who is actually providing the access
- The ability to record approvals and denials, including who did the approving or denying

The principle of least privilege

In security, the *principle of least privilege* states that personnel should have access only to the information or areas they require to perform their job functions. You need to apply this principle to your physical security systems.

Change Management

Like user access management, you need formal processes for the establishment and maintenance of security zones. The settings for each zone (and each door within the zone) need to be formally documented, periodically reviewed, and any changes to any door or zone configuration should be run through a process in which each change is reviewed and approved before it is carried out.

Handling Common Issues

A lot of issues need to be properly addressed in order to maintain a high level of security. This section covers the common issues.

Employee terminations

It is important to implement an effective user-termination process, to make sure that user access is being terminated promptly and completely. You need to retrieve access cards and deactivate them.

While it is important to deactivate a terminated employee's access in the system, it is equally important to preserve the terminated employee's history of events in the system, to support possible future investigations. Deactivate, don't delete.

Lost cards

Employees must be expected to immediately notify the physical security department if they have lost or misplaced their key card. Not only will this prevent someone who finds the card from using it before it is deactivated, but this will also prevent employees from using their

cards after they have claimed to lose them, as well as eliminate a spare they could give to a third party.

Organizations suffering from too many lost cards should consider assessing employees for all or part of the cost of replacing lost cards.

Forgotten cards

For a variety of reasons, employees sometimes forget to bring their cards to work ("the dog ate it" may still be a common excuse). Organizations need to have procedures in place to deal with this situation.

Nonclosing doors

In larger office buildings with centralized heating, ventilation, and air conditioning (HVAC), changes in air pressure sometimes prevent security doors from closing all the way. This can cause a door-propped-open situation, allowing someone to enter those doors without scanning their key card. It is important that these doors be adjusted to close properly as soon as possible, as well as be monitored so the physical access control system can detect this.

False intrusion alarms

Some doorways are more prone to false alarms, especially when *request-to-exit devices* (motion sensors placed on the interior side of security doors) don't scan a wide enough area. Here's what happens: If an employee is approaching a door to exit and the request-to-exit sensor doesn't detect the employee's approach, then the security system will think that door was forced open from the outside and trigger an alarm. To reduce false alarms in doorways where this occurs frequently, consider using multiple request-to-exit motion detectors with a wider "visual" range, a

request-to-exit button switch, or a crash bar or door latch with an integrated request-to-exit switch.

Monitoring the System

A physical security system can only be expected to effectively protect an organization if security personnel are paying attention to the status of the system at all times. Depending on the size of the organization, it may be one employee's part-time task to monitor the system, and in larger organizations this may be the responsibility of an entire department.

System event logging

A physical security system needs to have the ability to record all significant events, including but not limited to:

- **Successful entry.** Every employee entry to any area should be logged.
- **Unsuccessful entry.** Every "Access Denied" event must be logged. These events should be followed up promptly to determine whether an employee is attempting to access a restricted zone or whether a would-be intruder is attempting to gain access using illegitimate cards or codes.
- **Impossible activity.** Because it is physically impossible for someone to be in two places at once, logs should be monitored for multiple entry events on distant doors. This is the easiest way to identify a cloned card in the system.
- **Reader tampering.** For systems that include card reader tampering detection, the system should be logging all attempts to tamper with or remove card readers.

- **Equipment faults.** Malfunctions of any device in the system should be logged. This will help to detect equipment that may not be working properly, as well as possible signs of tampering.
- **Power failures.** Depending on the backup power systems, a power failure may be a critical event.
- **Employee card access changes.** All changes to employee access rights must be logged.
- **Zone configuration changes.** All changes to the configuration of security zones must be logged.
- **General system configuration changes.** Any change made to the overall configuration of the system must be logged, including the identity of the person making changes.

Critical events

The purpose of monitoring is to become aware of events in the physical security system that warrant action. The most critical events that require immediate response include

- **Tampered reader.** If tamper-detection alarms are triggered, this may indicate that an intruder is attempting to gain access to a facility. It could also be a sign of construction or maintenance.
- **Forced doors.** Any event where the combination of request-to-exit device, door status, and key card system indicates that a door was opened from the outside without a key card may represent a forced entry or an equipment malfunction.

- **System abnormalities.** Problems including "Reader offline" as well as system malfunctions and lock-ups require immediate investigation. They could indicate a tamper or intrusion attempt.
- **Network intrusion.** Firewalls and network intrusion detection systems that protect the physical security system may detect an attempted or even a successful network break-in. This may be an emergency situation requiring a temporary shutdown of the physical security system.

When a "bad card" is presented to a reader, some access control systems can record additional details. When an illegally obtained card is used and the message generated by the access control system is "Card out of range" instead of simply "Denied," it signals an urgency to investigate. Similarly, messages that note the use of cards that have the wrong data format or the wrong facility code should be taken as indicators that a foreign, illegally obtained card is being used.

Monitoring responsibilities and processes

A person, team, or department in an organization should be formally designated as being responsible for monitoring the physical security system. The job descriptions for one or more positions will include statements describing responsibilities for monitoring.

The process of monitoring itself should be documented. This includes general duties such as the systems and methods used to perform physical security system monitoring, as well as specific procedures for responding to each type of event.

Physical examination of readers should be included on guard tours. Look for stripped screws or anything altered or unusual.

Educating Employees

Educate your employees. By helping employees understand why security is important, and showing them how to use the system, they are far more likely to help use the system to protect themselves and your organization's assets. Some important points:

- **Don't prop doors open.** Doors should never be propped open. If there is construction, remodeling, or a lot of equipment being moved through the building, the facilities management team should make appropriate arrangements to provide supervision of open doors or prevent their propping altogether.
- **Do not tailgate.** For organizations that have a "one card, one entry" policy, it is important that employees understand that *tailgating* (following someone in without using their own card) cannot continue.
- **Avoid courtesy door holds.** It's nice when employees help one another, and holding doors open for others is still in style. However, this can't be done in facilities with "one card, one entry" and "badge in, badge out" policies. In order to be polite, offer to hold a door once an employee has badged in.
- **Do not loan or borrow cards or PIN codes.** While loaning IDs is a long-held (although illegal) tradition in many cultures, this has no place in organizations that are serious about their security.

- **Report lost or stolen cards immediately.** Anyone whose security card has been stolen or misplaced should report it immediately to the person or group that manages cards. It would be far better if a card indicated lost is later found than a situation where a stolen card is used by an intruder.

Regular System Reviews

Periodic reviews of security systems, which need to include physical security systems, are a common practice. Table 2-1 includes recommended activities that fit most organizations.

Table 2-1 Recommended Reviews

Activity	*Monthly*	*Quarterly*	*Annually*
Formal security assessment			X
Review security policies and procedures			X
Review access zone configuration			X
Compliance reporting		X	
Review user access		X	
Inspection of card readers, door contacts, request-to-exit devices, locks, and so on	X		
Review administrator access	X		

Chapter 3

Ten (Or More) Best Practices for a Layered Approach to Security

In This Chapter

- Improving your organization's physical security

This chapter offers several best practices for layering a security system.

- **Align security objectives with organizational goals.** A good security program will align with and support the overall organization's goals and objectives.
- **Conduct periodic risk assessments.** This helps to identify new threats in the environment.
- **Choose a quality security partner.** Although choosing the right security technology is important, it's even more vital to partner with a trustworthy and proven security vendor, one with a history of product quality and innovations. Look for certifications and credentials such as ISO 9001, UL 294, UL 1076, FIPS 140, FIPS 201, GSA APL, FCC, C-TPAT, CE, and ROHS. Seek a full-service

organization that can not only sell its equipment, but can support and help train administrators and users on the system as well.

- **Use smart cards.** Use of smart cards is, well, smart. They are powerful, secure, versatile, durable, and cost-effective. Most importantly, they enable a high level of security features, such as card-and-reader mutual authentication.
- **Use cryptography.** Military-grade, vetted cryptographic techniques that enable encryption and other security features are available for use in commercial products. Seek them out. Ideally, your facility's encryption keys should be unique from the vendor's other customers. And each of your cards should contain a unique diversified key.
- **Watch the logs.** A good physical security system is only as good as its management. This means scanning the event logs to look for unusual activity, including repeated attempts by people to enter forbidden areas, reader malfunctions, and door alarms.
- **Protect the wiring.** Exposed or unprotected wiring can be a major weakness in a physical security system. If an intruder is able to eavesdrop on reader wiring, he may be able to "replay" a valid key card and gain entry to a sensitive area. If an intruder can get to the lock wiring, he may be able to cause the door to release on command. The best bet is to place all wiring to host computers, panels, readers, locks, and status sensors in conduit, or way out of reach.
- **Make equipment tamper-resistant.** While it's relatively easy to protect controllers and related systems by locking them away in secure rooms, readers are "out there" — exposed to all employees and

maybe even the public. Making readers tamper-resistant and choosing readers that report tampering will help to prevent and detect tampering, making it harder for an intruder to break in to your facility.

- **Integrate with video and door status systems.** An effective physical security system will combine a key card system with video surveillance and door status sensors. This can help to detect forced doors and propped doors, and will give you an opportunity to get a visual read on the activity going on at your entrances. Set up your video system to capture a snapshot or short video clip of each door transaction (access granted, access denied, wrong PIN, bad card, and so on).
- **Use multifactor authentication to access higher security zones.** With even the best access card technology, a lost card could be used to enter a facility, unless multi-factor authentication is used. The use of combined key card and PIN pads, or key card and biometric readers, gives you extra confidence that the person using the key card is actually the person you issued it to and not someone who found it in the parking lot.
- **Educate your employees.** A physical security system is a "high touch" system that everyone uses. By helping employees understand why security is important and by showing them how to use the system, they are far more likely to help use the system to protect themselves and your organization's assets.
- **Prevent anti-passback.** To better control access to your facility, you can design your system with both "badge in" and "badge out" requirements. This will prevent someone from entering a facility

when the physical security system thinks the person is already there. This can help prevent the use of cloned cards as well.

- **Integrate with network directory services.** It's a lot of work keying all the users' names into an access control system, and it's tedious to maintain all the access rights. If you can integrate your system with a network directory service, such as LDAP (lightweight directory access protocol) or Microsoft Active Directory, then physical access can become as easy as associating people with access rights within the directory service, instead of doing it separately. And if, for example, your human resource system is also tied in, then when a person is hired or fired, the person's credentials can be added or revoked instantly without having to do it via another system.
- **Stay vigilant.** In the security business, security is never "done." Rather, we implement security controls, and then we monitor them, look for weaknesses, and make incremental improvements in the system. By adopting a mindset of continuous improvement, you can stay one step ahead of intruders who try to get around your system.

Now, the future really is wide open.

Introducing iCLASS SE™, enabled with the Secure Identity Object (SIO) model.

HID®

More portable, more flexible, and more secure than ever before. iCLASS SE — the platform that simplifies everything.

Products with this logo are enabled with HID's Genuine Secure Identity Objects/Processor Technology, delivering security and portability to your access management system.

hidglobal.com