SPONSORED CONTENT

CSO FROM IDG

HID

Want a Future-Proof Cyber Security Strategy? **Look at Physical Security Now.**

IT teams need to collaborate with their physical security counterparts to choose a solution that complements cyber security while providing scalability and ease-of-use.

FOR ANY ORGANIZATION, providing sound defenses against security threats to IT resources requires collaboration between the team responsible for cyber security and the team focused on physical security. If the door to your server room or data center isn't physically secure, neither are your IT resources. It's certainly a risk that security professionals are attuned to, according to a recent Ponemon Institute study. The study found 42% of security professionals are concerned about their organization's inability to secure physical spaces containing critical data.

A fully secure digital posture considers both network and physical security, along with user convenience, risk mitigation, and scalability. It's also important to take advantage of opportunities to integrate physical and IT security, creating a holistic approach and positioning the organization to future-proof system capabilities.

By evaluating physical access control alongside IT systems, organizations are able to address the dual challenges of fast-moving technology and a fast-moving threat landscape to bolster cyber security through physical security approaches.

42%

OF SECURITY PROFESSIONALS ARE CONCERNED ABOUT THEIR ORGANIZATION'S INABILITY TO SECURE PHYSICAL SPACES CONTAINING CRITICAL DATA.

SOURCE:
Ponemon Institute study

Factors Driving the Need for a Holistic Security Approach

Too often, physical security is a weak link, one that threatens the overall security posture of the organization. When an attacker has physical access to IT resources, even the most sophisticated cybersecurity controls can be bypassed or rendered useless. So-called "TEMPEST" attacks, for example, can decipher encryption keys by listening to electromagnetic emanations from a computer, using an inexpensive device that's small enough to be hidden inside a piece of pita bread.

The increased use of operational technology (OT) in various business areas—from manufacturing floors to office spaces—also presents new physical security challenges. OT includes everything from controllers on factory floors to smart building systems that manage lighting and HVAC in office environments. These networked sensors and control devices are at risk of tampering if someone with malicious intent has access.

How do organizations meet present needs for security while readying for tomorrow's demands?

Two Joint Actions with Physical Security to Boost Network Security Now

Giving physical security professionals a seat at the table is integral to thwarting insider attacks and other physical security breaches that can result in damage to IT systems. Moving to newer, more dynamic physical access control systems with greater efficiency and a more convenient user experience helps deliver a higher level of security over systems that are too hard to use or easy to breach.

"A digital security posture that doesn't account for physical security isn't taking a holistic approach," says Keith McNeil, Senior Director of Information Security for HID Global. "A comprehensive, risk-based approach which considers current threats and new technologies should be regularly performed to shape security architectures, and it is critical that physical security is part of this assessment."

ALLOCATING A SMALL FRACTION OF THE IT UPGRADE BUDGET COULD PAY FOR A COMPREHENSIVE PHYSICAL SECURITY UPGRADE THAT WOULD ADDRESS WEAK LINKS IN OLDER PHYSICAL ACCESS CONTROL SYSTEMS (PACS) AND SUPPORT NETWORK SECURITY EFFORTS.

ADD PHYSICAL SECURITY TO IT UPGRADE LIST

One such opportunity is when a company is in the midst of an overall risk assessment or IT upgrade. It's not uncommon for a company to execute yearly risk assessments and spend millions on company-wide IT upgrades but fail to consider physical security. Allocating a small fraction of the IT upgrade budget could pay for a comprehensive physical security upgrade that would address weak links in older physical access control systems (PACS) and support network security efforts. Opportunities include:

- **Upgrading from low-frequency (125 kHz) proximity cards and mag stripe cards**, both of which are vulnerable to interception and cloning. This could include the use of high-frequency credentials such as Seos® that enable secure identities not only for cards, but on mobile devices, wearables, and other form factors that are less likely to be left at home or to go unreported for days or weeks when missing.
- **Promoting the use of modern protocols**, such as Open Supervised Device Protocol (OSDP). Many PACS card readers use the Wiegand protocol for door to controller communication. Created in the early 1980s, Wiegand communications are unencrypted and vulnerable to interception and cloning.

- **Replacing physical credential management with a digital process for quick response to security issues**, such as deactivating devices and deprovisioning credentials over the air. Mobile credentials can be issued and updated electronically while eliminating the costs and time lags of reissuing plastic cards.

RECOGNIZE PHYSICAL SECURITY AS YOUR FIRST LINE OF DEFENSE

If an attacker successfully gains entry to a server room or data center, he can install malware or devices to capture confidential, sensitive data—or even bring down the network entirely. Physical security can mitigate these risks and further strengthen cyber security. Ways to address these risks consist of:

- **Combating malicious and inadvertent insider threats with physical security tools such as cameras and location-based monitoring systems.** Malicious insiders who have legitimate access to some areas of the building may be motivated to cause disruption or derive financial benefit by infiltrating systems or installing eavesdropping equipment. Alerts and alarms can notify security teams when occupants enter restricted areas without authorization and help protect against attacks on OT systems and sensitive IT resources.
- **Managing visitors by moving away from paper rosters and toward more advanced systems that integrate with PACS to grant access only to certain areas.** In addition, location-based monitoring systems work together with PACS to help ensure visitors don't enter restricted areas while also providing a record of where they have been in the building.
- **Converging physical and logical access can disrupt attackers who enter buildings by counting on the courtesy of others, such as a legitimate employee holding open a door.** Digital certificates loaded onto smart card credentials can ensure trusted login to networks, making it more difficult for bad actors to breach the network or plant sniffing devices.

Top Considerations for Future-Proof Security

As they explore physical security options, IT and physical security teams should keep in mind a number of key issues, including:

- **SECURITY:** First and foremost, of course, is security from both the physical and IT points of view. That's the ultimate goal. Be cognizant of physical security solutions that are too easily compromised, such as older PACS cards that can be cloned or hacked.

- **SCALABILITY:** A new PACS solution should be highly scalable, especially if you expect your facilities will expand as the organization grows. The ability to easily onboard or deprovision credentials helps in that regard. Rather than having to issue hardware tokens to each new user, they can use mobile devices they already have, such as a smart phone or watch. Biometric systems, likewise, use fingerprints or facial recognition technology for authentication.

- **CONVENIENCE:** Millennials are already highly mobile, and "Generation Z" employees will begin entering the workforce around 2020. These digital natives have grown up with smart phones and iPads and expect their mobile devices to hold the keys to just about any kingdom. A PACS solution that uses a smart phone or wearable as a form factor will be natural for them—and likely more convenient and secure for everyone.

- **FLEXIBILITY:** A PACS solution that supports multiple form factors is also more secure, because users are not likely to forget a device like their phone or smart watch—and certainly not their finger—and thus won't be tempted to try to thwart the systems. Such solutions also help position IT as the customer service organization many are striving to be.

- **INTEGRATION:** Consider, too, whether you want your PACS solution to integrate with IT systems (to provide network access, for example). Some organizations are looking to converge their physical and logical IT access solutions, and to create a single identity for each employee that covers both.

The Benefits of Physical and IT Security Collaboration

Providing a truly comprehensive security strategy requires getting IT and physical security teams to collaborate on a plan. That will help ensure physical security is considered as part of an overall risk assessment and aligned to business goals, receiving top-down buy-in. Such a strategy provides business benefits including:

- **Identifying suspect systems:** A comprehensive assessment will determine when physical security systems were last upgraded; whether the organization is using systems that are vulnerable to interception, cloning, or other threats; and provide more granular control over who can access what resources.
- **Keeping physical security in sync with IT:** Collaboration between teams can also help ensure that systems procured are in sync with the overall requirements of the organization, such as the ability for both physical security and network access and authentication.
- **Sharing information and creating a cohesive organization:** A team driving toward the same goals is able to break down silos, becoming strategically aligned and delivering a higher ROI to the business.

A Coordinated Approach to Overall Security Posture

Organizations of all stripes are rightfully hard at work trying to improve their IT security posture and fend off proliferating cyber threats. Too often, though, they overlook the role that physical security plays in that effort.

If your organization fits that description, it's time to take a hard look at your PACS solution and assess whether an upgrade is due—or overdue—and act before rather than after a breach. When doing so, make sure both your physical and IT security groups are at the table. Sharing plans and goals will ensure that PACS upgrades reinforces network security for a comprehensive program.

HID Global iCLASS SE® Readers

HID Global can help you find a PACS solution that will meet both your physical and cyber security needs, without sacrificing security or convenience. To learn more, visit **www.HIDglobal.com/access-control**.

IDG Communications, Inc.