Predicting Breaches
PIAM can find and stop insider threats

CEO Checklist
Is your firm doing all of these things?

Weak Links
How not to be a system's vulnerability

SIA Technology Insights

Special Cybersecurity Edition

Volume 4, Issue 1
Spring 2016

Welcome

Dear Reader,

After Jack Nicklaus won the 1965 Masters Tournament with a then-record 17-under-par, Bobby Jones, who up to that point was regarded as the greatest golfer who ever lived, said, “Nicklaus plays a game with which I am not familiar.”

Some professionals in the electronic physical security industry – especially those who started their careers more than a few years ago – may feel a similar unfamiliarity when they look at the most technologically advanced systems today. Everything is on the network, and computers and data now have as much to do with securing a facility as cameras and card readers. The physical location cannot be secure unless the network is – and vice versa – which is why this edition of *SIA Technology Insights* is devoted entirely to cybersecurity.

Soon, there will be no meaningful distinction between physical security and cybersecurity in this industry. The lines, as the articles herein make clear, have already blurred, and the Security Industry Association is moving aggressively to lead the industry into this new era, with the creation of the SIA Cybersecurity Advisory Board, two members of which contributed to this publication.

IP-enabled devices make security systems more robust, yet, often, also more complex. We hope the information that follows will help you to become more familiar with the latest trends and technologies and enable you to develop and implement the most effective solutions. We welcome your feedback and encourage you to contact the *SIA Technology Insights* editor, Ron Hawkins, at rhawkins@securityindustry.org with comments, questions or article suggestions.

Thank you for reading.

Sincerely,

Denis Hebert
Chairman, Board of
Directors
Security Industry
Association

Don Erickson

Don Erickson
CEO
Security Industry
Association

How to Navigate Through the Magazine

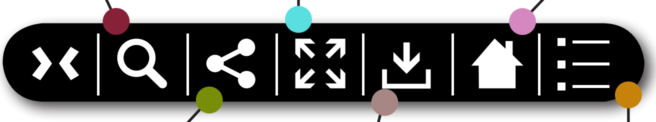
Navigation Bar

Click the arrows button to expand or contract the navigation bar.

Click the fullscreen button to view page.

Click the home button to go back to the cover of this Magazine.

Click the search button to look for keywords.



Click the share button to upload content on social networks or to email.

Table of Contents

Share:

What's New on the Video Surveillance Front? 6
By Fredrik Nilsson
A keener eye, a longer memory and a sharper IQ

Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security 12
By John Romanowich
As technology advances and prices fall, thermal cameras have become a cost-effective way to secure the perimeter.

Video Analytics in the Modern Security Industry 16
By Brian Karas
Analytics can make cameras smarter, but how smart can they get?

The Untapped Benefits of Recorded Video Surveillance 22
By Rafi Pilosoph
Recorded video holds a wealth of information that can be used not only post-event but also proactively. Fast video review makes accessing the data possible.

The (Slow) Transition to IP in Fire and Life Safety Devices 26
By Christopher Peckham & Walter Frasch
Codes and regulations often force fire and life safety equipment to use older technology, but that is changing.

Electronic Security Meets the Ecosystem 32
By Pedro Duarte
IP devices increase both rewards and risks. How secure is your security system?

Security and Privacy in a Connected World 38
By Kathleen Carroll
With proper planning and precautions, security and privacy can complement – not compete with – each other.

The Technology Behind TWIC 44
By Walter Hamilton
Smart cards are finally getting smart readers, but how will it all work, and how will it connect with existing PACS?

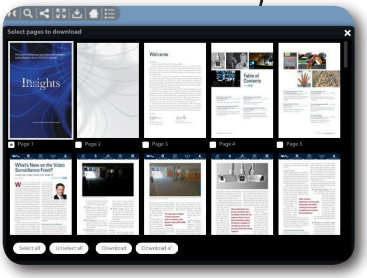
A Case for a Green Security Landscape 50
By John Hunepohl & Aaron Smith
Sustainability can be good for both the environment and the bottom line.

4 | SIA Technology Insights

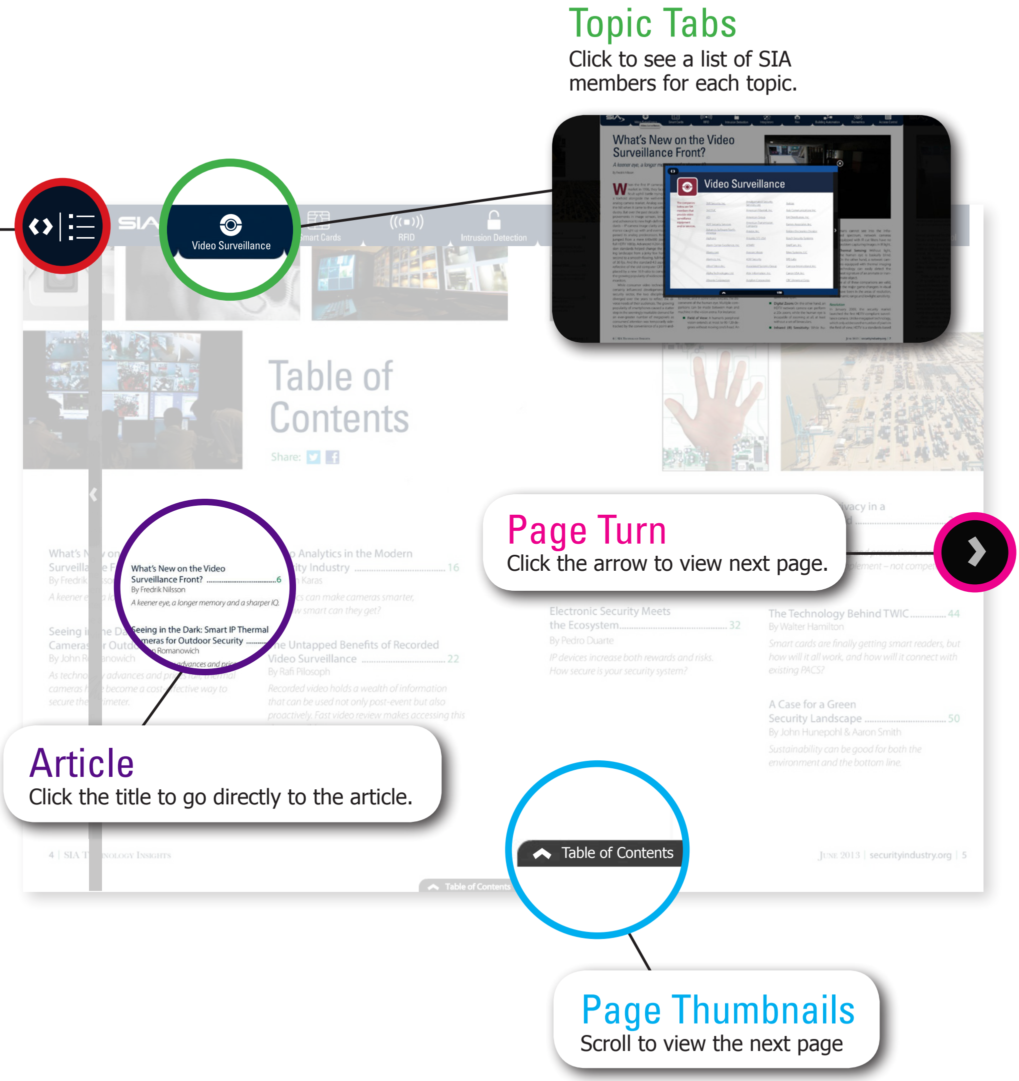
June 2013 | securityindustry.org | 5

Table of Contents 4-5/98

Click the bullet button to go to the table of contents.



Click the download button to save a PDF of the Magazine or selected pages.



Topic Tabs

Click to see a list of SIA members for each topic.

Page Turn

Click the arrow to view next page.

Article

Click the title to go directly to the article.

Page Thumbnails

Scroll to view the next page

What's New on the Video Surveillance Front? 6
By Fredrik Nilsson
A keener eye, a longer memory and a sharper IQ.

Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security ....
By John Romanowich

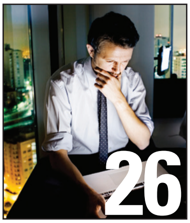
The Untapped Benefits of Recorded Video Surveillance 22
By Rafi Pilosoph
Recorded video holds a wealth of information that can be used not only post-event but also proactively. Fast video review makes accessing this

Electronic Security Meets the Ecosystem....32
By Pedro Duarte
IP devices increase both rewards and risks. How secure is your security system?

The Technology Behind TWIC....44
By Walter Hamilton
Smart cards are finally getting smart readers, but how will it all work, and how will it connect with existing PACS?

A Case for a Green Security Landscape 50
By John Hunepohl & Aaron Smith
Sustainability can be good for both the environment and the bottom line.

Table of Contents



52

60

70

78

SECURITY
86

Ultimately, protecting the most important asset of any company – its people – requires a combination of physical security and cybersecurity. Integrating the two will allow companies to more effectively maximize the strengths and minimize the weaknesses of both while creating a safe, secure, efficient, interconnected and fully automated environment.

IoT Makes New Security Partnerships Essential

Bringing physical security and IT security together can enhance both

By Rob Martens
Allegion

For several years now, security professionals have been a part of a remarkable convergence of two worlds – physical and digital. Security systems integrators are shifting from being strictly focused on hardware and electronics to taking into account services, software and networks, and security purchases are increasingly being rolled into IT because the hardware solutions need access to the network. The resulting turf battles have been as predictable as they are heated, with facility managers and CIOs each struggling to do what they think will be best for the facility and its occupants.

But while those battles are being fought, there is another, even bigger, shift that is just beginning to ripple through not just the security industry, but the entire world. The Internet of Things, or IoT, is not just a new trend, it is the next evolution in the revolution that began with the invention of the Internet. It represents a fundamental change to the access control industry that not only affects the kinds of tools we use and how we use them, but also who makes the decisions on the customer side of the table. Most

importantly, it is disruptive, in the best and worst possible ways, and we have only just begun to see its potential impact on our lives. Security dealers and integrators have a major role to play here as industry knowledge is critical to preventing consumer exposure to unforeseen difficulties and dangers.

Industry knowledge is critical to preventing consumer exposure to unforeseen difficulties and dangers.

What is the IoT?

The phrase "Internet of Things" was coined by British tech pioneer Kevin Ashton in 1999. The simplest definition and vision of IoT is that billions of sensors and smart devices will connect and share information with each other to enhance the collective experience of the end user. This is done by collecting, cleaning and analyzing the data provided. This, then, allows for predictive and real-time actions to take place on behalf of the user and the associated community.

It helps to think of IoT as the Internet itself, evolved for a third time. In the first two evolutions (or waves) of the Internet, people were connecting via either a desktop computer or laptop or on a mobile device, like a smartphone or a tablet. In the third evolution, smart devices will communicate and deliver information to the Internet without human intervention on a scale that has never been seen before. By the years 2020-2025, it is projected that there will be as many as 50 billion connected devices operating on the planet, generating data in volumes previously unseen.

Irrational Exuberance and (Not So) Irrational Fears

As with any new technology, IoT has given rise to both exuberance and fear. It has become a megatrend, and investors are willing to place significant bets on the perceived desires in the marketplace.

Being able just to connect a product to the Internet is no longer sufficient, and the ability to make a connected security device does not necessarily mean that a company understands how to effectively apply this new technology. A good example of this is the focus by some providers on the convenience of proximity-based auto-unlocking. In some cases, the wow factor has overshadowed the potentially dangerous exposure that comes with opening a door without a clear intent of some kind expressed by the user. The approach to these types of solutions differentiates the thought processes of a security and safety provider from those who see an opportunity but may not have the experience to identify the potential life safety implications.

At the other end of the spectrum are those who recognize that exponentially increasing the number of connected devices simultaneously increases the number of potential access points for hackers to exploit.

According to security industry analyst Gartner, the black market for fake sensors that would allow data to be compromised or manipulated will be worth upwards of $5 billion by 2020.

And hackers are not the only ones that consumers will need to worry may be spying on them. In February, U.S. Director of National Intelligence James Clapper told a Senate panel, “In the future, intelligence services might use the [Internet of Things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.”

When added to the almost daily announcements of the latest organization whose data has been hacked, from Target to Neiman Marcus to the U.S. government’s own Office of Personnel Management, all of this creates the not unreasonable impression that digital security solutions are less secure than mechanical ones. It is this public perception of the vulnerability of connected security systems that can create an even greater risk – inaction.

All or Nothing

It is easy to understand why many would feel as though there is not a connected system out there that is “fully secure,” so why spend money on any of them? Consumers are well aware of the risks associated with being an early adopter of any technology or product. No sooner do they invest their money in one item than a competitor will introduce a much better one that, of course, is not compatible with their system.

But doing nothing is not a plan for anything except failure. Instead, one must plan for everything to be hacked from the beginning of the selection process. For example, picking a lock is a hack, as is stealing and using a master key. What matters most is how quickly and effectively somebody is able to respond to the attack. In many cases, digital solutions can facilitate a faster and more robust response to these situations than a traditional mechanical lock or solution. If the master key is stolen, is it easier to physically rekey each lock, or is it faster and more efficient to change the firmware remotely controlling all of the locks at once with minimal touring?

All of these things must be considered when selecting a solution.

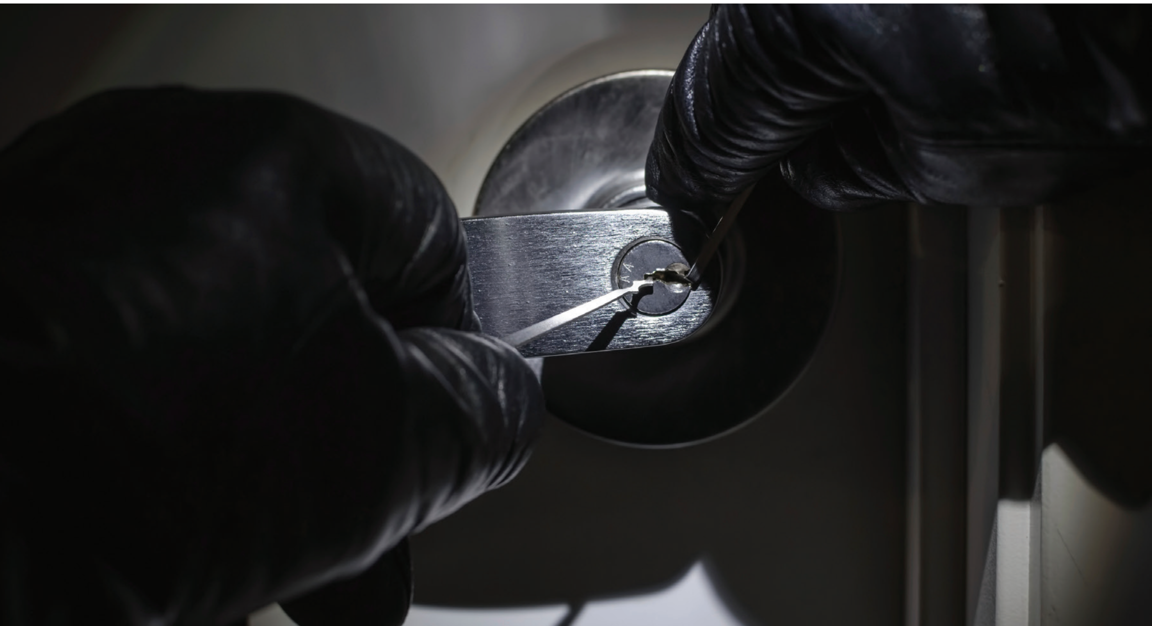
Getting past the inertia of indecision can often be managed through detailed communication and concrete information about how a building's systems can live side-by-side and how integration can benefit the customer in the long run.

Building Automation

The front lines of IoT in the security industry can be seen in building automation. Security integrators are realizing that there is a business opportunity in every building, and access control is just one piece of that potential business. This new technology is enabling the deployment of electronics within a building's ecosystem of services, from physical access control and logical access to lighting and HVAC systems.

Getting past the inertia of indecision can often be managed through detailed communication and concrete information about how a building's systems can live side-by-side and how integration can benefit the customer in the long run.

Consider a building where employees scan a badge or present a smartphone-based credential for access. When access is granted, the building's other systems are triggered to turn on the lights, adjust the temperature and alert security that someone has entered the building. During the day, the network monitors water use, sending an alert to facilities if a restroom faucet is left running or if a normally locked door is left ajar. At the end of the day, the access credential is used to exit the building, triggering



the reverse actions of the morning – lights are dimmed, temperatures are adjusted, doors are locked and security is notified. While access control may be the "trigger" for all of these functions, the entire system is based on a sophisticated network.

Every aspect of a building's operation ties into a network, including lighting, intercoms, access control, video, fire safety and climate controls. This is further driving the interoperability of these previously disparate systems to enable services such as location-based decision-making that will provide a new level of value to end users.

Creating ROI for End Users

In order to effectively sell a multi-part integrated network, it is critical to be able to pinpoint an end user's possible return on investment. This can be achieved by a detailed cost analysis that compares current use and expenses to the results that can be achieved through upgrading equipment and integrating technology:

- Upgrading to stand-alone intelligent controllers can reduce lighting expenses by as much as 40 percent.
- Buildings with strong southern light exposure can adjust HVAC and lighting based on actual conditions, rather than a fixed schedule, taking advantage of natural heat and light to reduce energy use.
- Buildings with door and window sensors can detect when doors and windows are open, signaling the system to automatically turn off the HVAC system while also alerting security personnel to a possible unauthorized entry.

These examples of ROI are significant whether customers occupy large commercial office buildings, health care clinics, restaurants, hotels or even manufacturing facilities.

Buildings waste a lot of energy. Just propping a door open can cause the HVAC system to go into overdrive, pumping out air and creating significant energy waste. The ROI on building automation can sometimes free up money for other projects while enhancing technology, comfort and security. This can be a game changer for customers in the education, health care and government markets.

When groupings of these smart devices work in unison, they can reveal previously unseen patterns and opportunities. This can generate huge opportunities and, in the case of the security industry, a much more personalized experience for the building user and greater efficiencies for the owner.

Changing Landscapes

Even as this technology is fundamentally changing the traditional boundaries of security, so too is it causing a shift in the decision-making authority from facility managers to IT leadership. This is a trend that began when companies migrated to IP-based video surveillance and access control systems, and IT managers became increasingly involved in physical security decisions. However, in many companies, there still remains a clear division between the physical access control and IT security departments, with little interaction between the two.

Facility managers are frustrated that they are expected to adopt the new IoT technology without much experience. They are also worried about the implications of this change, as they will ultimately be held responsible for it. The CIO is largely unfamiliar with the physical security implications and has serious concerns about the impact this technology will have on the network. Both parties are concerned that, when a building is fully automated and networked, a failure in one area can cause failures in others.

Security dealers, consultants and integrators have a critical role to play in this situation. Helping to create a working relationship between the CIO and the facility manager is crucial to the successful adoption of IoT in access control. Educating the CIO about physical security and bridging the knowledge gaps for the facility manager will be a key differentiator for successful dealers, consultants and integrators as the industry moves to a more IoT-centric mindset.

> *"As long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one. The convergence of cyber and physical security has already occurred at the technical level. It is long overdue at the organizational level."*
>
> *– Scott Borg*

Providers and integrators are the glue for the coming wave of IoT-enabled facilities. They should present themselves as a coordination point for IoT, where they act as knowledgeable, trusted mediators between the CIO and the facility manager. IoT implementation will move at the speed of that relationship.

Communication is Key

So how does one foster communication between the two worlds of digital and physical security?

- Start early. Make sure the leaders of both areas are involved from the beginning. This will set the tone for working together to jointly develop a solution.
- Make sure both sides have the opportunity to voice their concerns. This will give security the opportunity to understand IT infrastructure and how the addition of locks or cameras can affect the network. It will also give IT a better appreciation of the liability and reputation risks of not having a proper security solution in place.
- Speak both languages. Stay current on the latest fire, life safety and building codes and understand their implications on the products being specified or sold. At the same time, providers and integrators must be able to demonstrate to IT that they can speak their language and understand how the system is being utilized.
- Clearly identify capabilities. Several questions need to be asked, such as:
  - What IT security policies and standards are in place?
  - Can the system support security beyond PCs?
  - How is cabling installed?
  - Is the server environment virtual?

  - Do you maintain backups or do you want the integrator to do that?
  - How do you onboard a new application?
  - How do you want to handle maintenance of the security solution?
- Think long term. It is important to view the partnership beyond the basics of installation, implementation and maintenance. Consider how to partner throughout the life cycle of the security solution, three, five and even 10 years down the road. This will enable the solution to continue to be effective as security needs – and technology – evolve.

Building Successful Partnerships

Security projects are becoming increasingly complex, often requiring the expertise of several professionals, including architects, IT personnel and even device manufacturers. The challenge is bringing together all of the consultants and working collectively and collaboratively toward a common goal. Because technology, security hardware products and building codes change regularly, or have nuances to them, it is important that a large security project be approached from several angles. One individual or company does not typically possess all of the knowledge that any security project requires, but by garnering the collective brainpower of many advisers, the consultancy team can identify and develop the best solution for a facility today, as well as in the future.

As with any group project, communication is key to ensuring that there are no misunderstandings about who is responsible for what. Once the entire team is assembled, it is helpful to formalize the working relationship by developing an official statement of work that clearly outlines deliverables and expectations for each member of the team. This is also a good time to:

- Clearly outline the project scope
- Identify the expected deliverables
- Prioritize the key elements
- Develop a preliminary timeline
- Estimate a budget range
- Create a list of internal stakeholders

One of the most important decisions will be the selection of the right manufacturer. Security practitioners have the challenge of evaluating all of the people who present their solutions. Some will have incredible funding behind them, but inherent knowledge is crucial as there can be real dangers associated with some of these products. Companies that have experience partnering with other consultants and stakeholders – architects, integrators, IT, one-card providers, building owners, facility managers, etc. – to develop comprehensive solutions are often the best qualified.

Convergence

Many IT departments are

struggling to cope with the convergence of so many new technologies on their network infrastructure. In addition to traditional network security threats, they must now also monitor equipment such as HVAC systems and smart grid power monitoring and control devices, as well as IP-based access control systems and networked surveillance cameras, to prevent exploitation of these potentially vulnerable network nodes.

But connected security is also heavily dependent on physical security. An attacker gaining physical access to a terminal where a memory device can be plugged in is all that would be necessary to create a tool to be used in an attack. The lack of integration between physical and connected security creates a number of challenges that can be exploited.

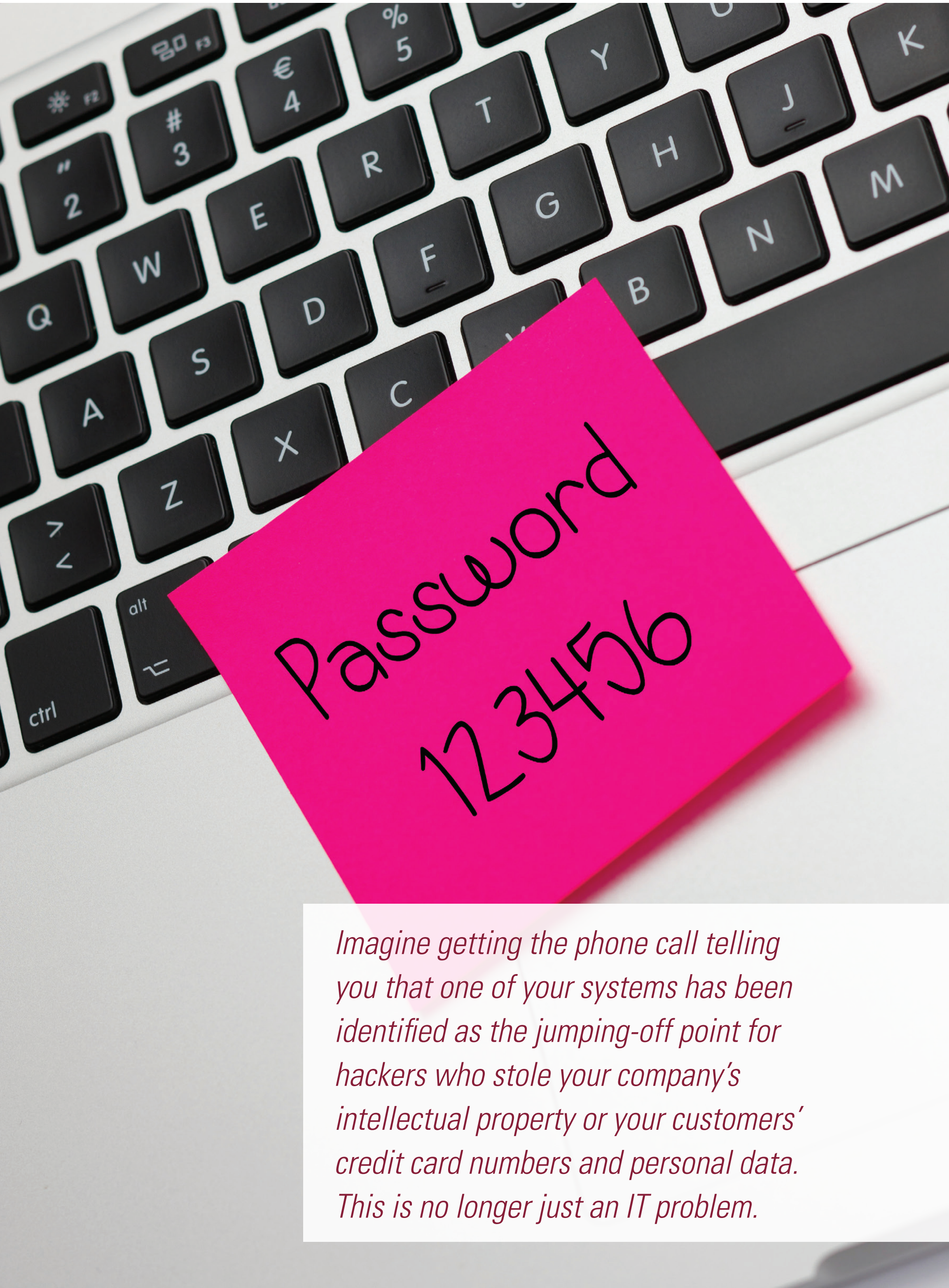
As Scott Borg, director and chief economist of the U.S. Cyber Consequences Unit, recently commented, "As long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one. The convergence of cyber and physical security has already occurred at the technical level. It is long overdue at the organizational level."

Ultimately, protecting the most important asset of any company – its people – requires a combination of physical security and cybersecurity. Integrating the two will allow companies to more effectively maximize the strengths and minimize the weaknesses of both while creating a safe, secure, efficient, interconnected and fully automated environment.

Some of these technological changes will occur rapidly, while others may take years to be fully implemented. If the speed of adoption of connected electronics and IoT is to increase, it is vital that people who understand the core elements of physical access control lead the application of these new tools wisely. With the proper focus, this technology can be adopted safely and will generate great benefits. ■

Back to TOC

Rob Martens (robert.martens@allegion.com) is the futurist and director of connectivity platforms at Allegion (www.allegion.com). ✉



Imagine getting the phone call telling you that one of your systems has been identified as the jumping-off point for hackers who stole your company's intellectual property or your customers' credit card numbers and personal data. This is no longer just an IT problem.

Because You Can Never Be 100% Cybersecure

Effective use of strategies for countering attacks can minimize risk

By James Marcella
Axis Communications

When was the last time you changed your password for your online bank account? Your email? Your social media accounts? How about your online shopping accounts or the myriad other login credentials that make up your digital life? Has it been a few months? Maybe a year? Hopefully, it has not been longer than that.

This article is not meant to be a treatise on password protection, but rather a wake-up call for security professionals who are used to evaluating risks in terms of probability and severity. Specifically, the article will urge you to apply your current knowledge of risk assessment to an area that is traditionally the responsibility of others in the organization. You may have procedures or policies in place to protect your personal data, but you can no longer afford to ignore the possibility of a cyber breach. You need to calculate what the potential impact to your organization would be should one occur.

Two converging trends are escalating the urgency. First, next-generation electronic security devices continue to migrate to the IP backbone, following in the footsteps of the consumer electronics industry and the Internet of Things (IoT). Second is the growing prevalence of "bring your own device" (BYOD) policies at many organizations, which increase areas of exposure to cyber threats.

> *Systems can only be made more secure by adding layers of measures and policies that minimize exposure opportunities and thereby reduce risk. In other words, cybersecurity equals risk management.*

So the question you should be asking yourself is whether the devices that you are responsible for are actually secure. If not, the consequences could be devastating. Remember the Target breach that ended up costing the company more than $252 million and doing immeasurable damage to its reputation? That attack was initiated through the company's HVAC system.

Imagine getting the phone call telling you that one of your systems has been identified as the jumping-off point for hackers who stole your company's intellectual property or your customers' credit card numbers and personal data. This is no longer just an IT problem, nor should you want it to be because it might affect your ability to choose the best solutions for you to protect people and assets.

How Best to Approach Cybersecurity

For starters, cybersecurity is more than a product. It involves people, processes and technology across the entire vendor supply chain, as well as the end user organization. Threats must be managed on a systems level, as it is rarely just one product that is breached; typically, several across an organization's infrastructure fall victim.

For example, a camera or other edge device might be the entry point rather than the ultimate goal of a hacker. Outdoor cameras, in particular, present an interesting challenge as they provide a wired connection to an internal network that could easily be exploited if proper security measures are not in place. These measures range in sophistication from basic tamper-resistant enclosures to advanced port-level authentication at the switch. There are multiple options between these two extremes, which gets to the heart of the matter. When it comes to cybersecurity, there are no totally secure systems. Systems can only be made more secure by adding layers of measures and policies that minimize exposure opportunities and thereby reduce risk. In other words, cybersecurity equals risk management.

Start with Cyber Risk Analysis

A cyber risk analysis will determine the probability of loss to an organization so that an educated decision on mitigation factors can be made. To understand the full implication of cyber risk, three questions should first be considered:

- Who are the potential attackers?
- What are their targets?
- What will be the costs associated with a successful breach?

It is important to recognize that costs often extend far beyond the immediate financial impact. There is also the long-term cost of regaining public trust once an organization's reputation has been compromised.

One can also benefit from referencing several well-established models for analyzing security needs, such as the "NIST Cybersecurity Framework" and "ISO/IEC 27001 – Information Security." Both are great frameworks for establishing a proper cybersecurity posture for organizations of all sizes. Based on the results of the risk assessment, security professionals can opt for any of several approaches:

- Assume the risk, making the organization liable for any loss
- Mitigate the risk by taking action to reduce loss
- Transfer the risk by paying for cybersecurity liability insurance
- Avoid the risk entirely by not implementing the system

In most cases, the last option is not a viable alternative unless a different solution can be found that decreases the risk to acceptable levels.

Identify the Most Vulnerable Areas

Cyber vulnerabilities fall into three key areas:

- *Careless users* – those who do not follow policy and procedures or simply make a mistake
- *Exploitable systems* – components that have exploitable vulnerabilities or lack proper processes and policies
- *Flawed implementation* – solution designs and deployments that open the door for exploitation

Roughly 90 percent of successful breaches result from human error, poor configuration and poor maintenance. Attackers will always take the path of least resistance, which starts with the users of the system and graduates in complexity to implementation flaws. The most common user vulnerabilities include:

- *Social engineering.* A tactic that attempts to trick someone into providing information that can be used to gain access to network resources. This is the most common method of attack.

- *Bad passwords.* A constant threat as users balance their ability to remember a password against the ease with which it can be guessed or cracked using a brute force attack. In some cases, the devices on a network might not support strong passwords, which combine numbers, uppercase and lowercase letters, and special characters.
- *Phishing.* Attempts to gain sensitive information through electronic means by masquerad-ing as a trusted source. In many cases, this is done through e-mail solicitations.
- *Application installations.* Downloaded programs from untrusted sources that inject malicious code into a device.
- *Lost devices.* Unencrypted personal devices that are lost, stolen or surreptitiously cloned will always be a concern in the world of BYOD.

Hold Vendor Channels Accountable

Manufacturers and systems integrators need to be held accountable for introducing cyber vulnerabilities as well. It is not possible to create a 100 percent secure system – at least not a usable one. The best that can be done is to make the system more secure by reducing exposure areas and mitigating as many risks as possible.

Manufacturers cannot give any guarantees that their products, applications or services contain no vulnerabilities that may be exploited for malicious attacks. However, they have an obligation to develop products and services that contain a minimum amount of exploitable flaws.

Did you catch that caveat? "A *minimum amount* of exploitable flaws." Does that mean that manufacturers *knowingly* produce products with exploitable flaws? Yes, they do. And, in many cases, they call them features and benefits.

Look at network cameras, for example. They are purposefully designed to enable customers to load analytics and embed them on the camera. It is a great way for trusted developers to create solutions that provide real value to the security practitioner – applications such as people counting, object left behind, cross line detection and video motion detection. All of these are commonly deployed analytics that reside on the camera. That same processing capacity, though, could be used by a malicious

> *It is important to recognize that costs often extend far beyond the immediate financial impact. There is also the long-term cost of regaining public trust once an organization's reputation has been compromised.*

application that is loaded onto the camera from an untrusted source.

So, short of operating as an isolated silo, where does that leave you? Take heart, because manufacturers generally possess a solid knowledge base regarding cybersecurity that you can draw on for strategies to reduce risk.

It all begins with understanding what steps the manufacturer is taking to protect the products and systems in its portfolio. Five key areas, in particular, should be noted:

- *Platform and Firmware.* The firmware used in most network camera products is based on Linux. The open source community is constantly monitoring and updating both kernel and services when vulnerabilities and flaws are identified. Firmware should be developed with the latest applicable open source packages with a strong emphasis on "security as a priority," which ensures that the firmware and interfaces are robust and resilient. Before final release, the manufacturer should have reviewed, audited and tested the firmware using penetration/vulnerability scanning tools.
- *Systems Integration Interfaces.* Network cameras constitute one or more nodes on the network. This means they have to be compatible with the network infrastructure to which they are attached. Therefore, standardized network protocols should be used. Some examples of security-related interfaces are HTTP digest authentication, HTTPS, 802.iX, SNMP, SFTP, SSH and remote syslog.
- *Product Configuration and Management.* Surveillance cameras provide a number of services that can be configured for a wide range of systems. Some examples related to cybersecurity are least privilege accounts, ability to enable/disable services, IP filtering, system and access logs, and detectors such as tampering, reboot and malfunctions.
- *Content Protection.* Cameras generate video that may need to be protected for privacy and compliance with regulations. Examples are HTTPS (depending on the client capabilities), privacy masking and edge-storage encryption.

- *Support.* The manufacturer should have a history of quickly providing firmware updates when vulnerabilities are discovered, even for discontinued products if the vulnerability is considered to be a high risk. They should also publish CVE (common vulnerabilities and exposures) reports when vulnerabilities are discovered. These reports include a threat level analysis, short-term recommendations, and plans to mitigate risks.

Systems integrators and end users should evaluate a manufacturer based on these defined responsibilities as part of their risk analysis. This upfront due diligence could save a security professional's job down the line should a breach occur.

Two Kinds of Attacks: Opportunistic and Targeted

Most cyber breaches are "opportunistic" in nature. Hackers will try to exploit vulnerabilities to attack random organizations. If a selected attack vector fails, the attacker will move on to the next victim. This is a lot like hardening in the physical security world. All you need is to be harder to rob than your neighbor or to be able to run faster than your friend when a bear is chasing you. Opportunistic attackers prey on poorly configured systems.

A more sinister and potentially costly type of breach is referred to as a "targeted attack." In this case, motivated individuals, hacker groups, nation-states or even terrorists target specific organizations. These attacks typically involve intelligent planning and target specific users or system vulnerabilities to achieve a specified objective. The well-known breaches at Target, Sony and the U.S. Office of Personnel Management are examples of targeted attacks.

Understanding the type of threats a risk analysis exposes will help to determine what preparations and cybersecurity posture a given organization should take. Here are a few tips:

Once the risk analysis is done, an organization needs to raise user-base awareness of the threats and mitigating factors of potential cyberattacks. It should define a policy, set up procedures and then educate. At a minimum, it must make sure that employees choose strong passwords that include a mix of uppercase and lowercase characters, numbers and symbols. A good password management policy will stop most opportunistic attacks. The company needs to embrace a security culture across all levels. If employees report suspicious behavior such as "tailgating," shouldn't they do the same for possible phishing e-mails they receive?

Administrators of physical security systems need to take a proactive approach to cybersecurity on a much more granular level. Although every system's threat posture is unique, some foundational practices should be adhered to. The SANS Institute was formed in 1989 and is a leader in educating security professionals on information security. They have produced the “SANS Top 20 Critical Security Controls” for networked devices. This list includes:

- Inventory of devices and software used on the network
- Continuous vulnerability assessment and remediation
- Maintenance, monitoring and analysis of audit logs (per device)
- Limitation and control of network ports, protocols and services

Very few end users keep their products up-to-date with the latest firmware. In some cases, this is because of software incompatibilities between their systems. And rarely do they disable protocols and services like UPnP or Bonjour even though they are not being used.

Roughly 90 percent of successful breaches result from human error, poor configuration and poor maintenance. Attackers will always take the path of least resistance, which starts with the users of the system and graduates in complexity to implementation flaws.

Regular retrieval of system reports or audit logs seems to be a priority when there is an incident, but not prior to the event when they could have provided very useful information. To top it off, many companies do not maintain an accurate inventory of what products they have on their network. Sometimes, they find out only after an adverse event or device failure has happened.

A structured, proactive approach as defined by the SANS Institute can make a difference by focusing efforts on those activities that have the best return on investment based on the most common attack patterns.

Cybersecurity Must Be a Team Effort

All network devices are subject to threats, including network cameras. A network camera is always part of a larger system where the network is the backbone. All parts are vulnerable, either as a system or as individual devices, and the entire ecosystem needs protection.

Threats must be managed on a system-wide level, and the responsibility for securing the network, its devices and the services it supports falls across the entire vendor supply chain as well as on the end user organization. It falls across people, processes and technology. And it falls, especially, on the company’s security professionals. ■

Back to TOC

James Marcella (james.marcella@axis.com) is the director of technical services for Axis Communications (www.axis.com).

Organizations that allocate extensive security resources to monitoring physical and cyber systems often fail to prevent a crime from occurring. The focus must shift to prevention.

Becoming Predictive, Rather than Reactive

A holistic view of physical and logical identities can help to identify insider threats

By Don Campbell
Quantum Secure

Current events have raised awareness of digital threats worldwide, bringing cybersecurity to the forefront of our global consciousness. It seems that hardly a day goes by without news of an attack and precious digital assets such as personal and financial data being unscrupulously dispersed around the globe. Among the many responses to these incidents is the U.S. government's mandate for programs to thwart digital criminals.

Before digging into potential solutions for addressing these digital threats, it is important to examine the landscape to understand not only the digital world but the physical world as well – and how the two intersect with regard to cybersecurity.

Cybersecurity has become a part of nearly all of today's business strategies. This has led to a number of companies gaining traction with technologies that apply intelligence on top of infrastructure to harden networks and detect vulnerabilities to prevent breaches.

These cyber programs are an excellent start, but many fail to address a key element of the issue. Not all data breaches are committed by hackers in remote locations around the world. Sometimes, they come from within an organization, often from individuals who are authorized to have access to parts of the network, if not all of it. To fully comprehend cybersecurity and programs to detect insider threats, it is vital to have a complete understanding of the various individuals – or identities – within an organization. In this case, an identity is defined as a person or entity – an employee, contractor, vendor, temporary employee or visitor represented by records within the system. An identity record will contain information about an individual, including basic human resources data, such as home address and emergency contact information. It may also contain additional information used to authenticate that an individual is who he or she claims to be, such as government IDs, photos, biometric data and/or background check findings. Lastly, identity records often contain information about the assets or areas to which people should have access. In many organizations, there are two different types of identity records: logical and physical.

> *To fully comprehend cybersecurity and programs to detect insider threats, it is vital to have a complete understanding of the various individuals – or identities – within an organization.*

A logical identity consists of a combination of controls used for identification, authentication, authorization and accountability in computer information systems. These components enforce access control measures for systems, programs, processes and information and may be embedded within operating systems, applications, add-on security packages, and database and telecommunications management systems.

A physical identity, on the other hand, represents a set of credentials and attributes that define the physical presence and location of an individual and must be verified before providing physical access. There are a number of key attributes that define the physical identity of an individual, including badging and access credentials, personal data, HR information, background check findings, and training and certification records.

With both logical and physical identity types, it is necessary for organizations to establish a definition of trust. For example, what requirements must be met before a credential is issued to an IT manager who requires access to an organization's data center? Keep in mind that similar questions must be answered for every identity type that is issued, making this a daunting task. This is where technology becomes an essential tool, to organize and automate information while maintaining accuracy.

A policy-based physical identity

and access management (PIAM) system automates the workflows associated with onboarding all of the various identity types that are issued. Beyond automation, PIAM solutions also ensure that the right identity is given the right level of access to the right areas and assets for the right duration of time. To further deepen levels of trust for each identity type, additional controls are put in place, including background checks or biometric data for accessing highly secure areas.

Understanding the critical role a policy-based PIAM solution plays in automating the processes associated with applying specific levels of trust to specific identity types is an excellent first step. The next phase of securing both physical and logical assets is to gather security intelligence, specifically the ability to understand each identity's behavior across the entire enterprise.

Security Intelligence

So how is intelligence gleaned and applied to prevent threats? Say an employee who has worked from 9 a.m. to 5 p.m. in a specific building for several years starts exhibiting access patterns outside of that norm. This might be entering the building at odd hours, attempting to gain entry to areas where authorization has not been granted (such as server rooms), or downloading more information than usual from the network. Of course, this unusual pattern may be the result of a new position, a change in working hours, a particular project that requires temporary access to different areas or assets, or any number of other reasons. However, this change in routine could also mean that the employee is involved in something more nefarious, such as insider theft.

This is where security intelligence – more specifically, predictive analytics – enters the picture. If all of an organization's identity records are stored in siloed systems, there is no connection between, say, access control, identity management and HR data. In such environments, which are unfortunately fairly common, there is little or no opportunity to see a holistic picture of how an individual identity is behaving. As a result, organizations do not have a clear view of their potential exposure to risk.

The number of networked systems and devices is growing, generating vast amounts of data, so much that it would be impossible for any person, or even an entire department, to sort through to identify threats that would enable an organization to take proactive measures. However, there is a solution.

How PIAM Fits In

The first step in gleaning security intelligence is to establish a baseline with data and metrics, which will serve as the foundation for identifying any anomalous behaviors. In the case of the aforementioned employee who rarely deviated from the established routine and access patterns, if the physical security and IT departments had set their baseline data, the new actions would have raised red flags and alerted the appropriate parties. Now imagine that equipment or sensitive logical assets had been reported missing during the same timeframe as this change in behavior.

> *The focus of security is undergoing a significant shift, evolving from risk management to providing demonstrable value to an organization. No longer are security professionals risk mitigators alone. Rather, they are increasingly becoming key players in overall business strategies.*

With a predictive analysis solution in place, the employee would have risen to the top of an audit list. Say, for example, organizational policy dictates that a security officer be dispatched for a tour of the facility on the third instance of anomalous behavior. With this simple policy in place, and with background data in hand, the officer might observe the employee removing something from an area that the worker does not typically access.

This is a very simple example of the power of predictive analysis for an organization and is mainly focused on physical access. However, one of the main challenges with insider threats and cybersecurity is that no two breaches look alike. Therefore, more effectively identifying and potentially thwarting insider threats requires that physical and logical security work in tandem.

A Closer Look at Insider Threats

Data breaches can create staggering costs for an organization. For example, entertainment industry analysts estimate that, as a result of the 2014 breach related to the release of the film "The Interview," Sony lost somewhere in the ballpark of $90 million.

Of course, not all breaches come with such a high price tag. The majority of costs are assessed on a situational basis. For instance, if a sales representative copies a client list when leaving an organization to join a competitor, it would be possible to make a projection of the resulting loss in sales. Or if an employee who has been terminated deletes company files, the cost of identifying which files are gone and retrieving them from archives can be determined.

The cost of other situations may be

more difficult to calculate because of the complexity of the breach. A few of these examples range from the theft of intellectual property, including source code; the deletion or sabotage of source code; or the misuse of data, all of which could have potentially catastrophic effects on a business.

Insider breaches can take many forms. Over the years, the Software Engineering Institute's CERT division has put together a library of incidents, a few of which are listed below:

- A law enforcement professional stumbled upon a way to create fake driver's licenses completely by accident.
- A systems administrator who had been terminated was able to delete 18 months of cancer research because there were no access controls in place.
- The submission of $20 million in false health insurance claims was enabled by a developer who discovered a lack of oversight for certain business practices.
- A software project leader covered up an inability to meet deadlines by sabotaging a development project.
- A currency trader made unauthorized source code changes to cover up nearly $700 million in losses over a five-year period.

Unfortunately, but not surprisingly, the list goes on and on.

Integrating a Broader Range of Systems

Given the seemingly endless possibilities of insider threats, how can enterprises effectively reduce their risk and protect themselves from these types of incidents? The challenge is further compounded by the faulty logic many enterprises use in viewing breaches as isolated incidents when, in truth, they are culminating events that follow a pattern of activity across multiple systems. The key to combating insider threats begins with expanding the data sources that are employed to detect threats from all of the networked systems within the enterprise.

Perhaps the most crucial of these additional data sources is the human resources database, which lists individuals' job titles, roles and responsibilities, associated levels of access to data, and the results of any background checks. People who have access to data as part of their job may represent a higher risk, while lower-level employees who accidentally discover and access unprotected data might pose a much lower risk. For instance, the critical or sensitive data that can be accessed by employees who work in finance, engineering or IT has the potential to do more harm than the data most employees can access.

Other important information contained within the HR database are records of triggering events, which are those events that may serve as a precursor to an employee posing a higher level of risk. Examples include employees who have received negative feedback or a poor performance review; who scored poorly on a performance improvement plan; or who have been subjects of complaints or guilty of infractions. Other red flags HR records can track include changes in family status that could place additional hardships – financial and otherwise – on individuals.

Identifying those employees who may pose a threat requires the widest possible perspective. Enterprises must employ procedures and mechanisms to correlate HR information with other enterprise systems, including those that monitor access to physical facilities and logical assets. That way, if a "9-to-5" employee attempts to enter a facility late at night or starts frequenting a building where he or she has no responsibilities, those patterns can be flagged. The PIAM solution can then automatically cross-reference those deviations with HR data to determine if the unusual behavior is the result of a job change or other non-threatening reason, or whether it may be indicative of a potential insider threat.

In addition to HR, data from access systems must also be correlated with calendaring systems. If an entire team or department comes in at an unusual time, they may be preparing for a business trip, an upcoming conference or a teleconference with a client in Japan – all of which are perfectly acceptable and would be contained in the calendar system. But a single employee doing this would be much more suspicious and would warrant a closer look.

Companies can also use IT logging systems to identify unusual equipment usage patterns, such as employees using photocopiers, printers or USB drives more frequently than in the past, or using external data-sharing sites. All of these may indicate unauthorized collection of information in an effort to misappropriate data.

Today, the focus of security is undergoing a significant shift, evolving from risk management to providing demonstrable value to an organization. No longer are security professionals risk mitigators alone. Rather, they are increasingly becoming key players in overall business strategies. For every business unit, the reality is that having to explain what went wrong and how it happened is much more

costly than allocating funds to preventing incidents before they occur. Yet most organizations focus solely on the cyber component with no real understanding of the broader function of identity management.

High-security organizations spend a fortune each year on ensuring both physical and digital security through the use of access systems, security operations centers, alarm management, and surveillance and other security monitoring, as well as a large team of security personnel. While most of that spending is on reactive real-time systems, real-time monitoring can only have a positive impact if it enables sufficiently rapid detection, analysis and dispatch to stop incidents. Unfortunately, the response window in which real-time monitoring can prevent loss is rather small, measured in minutes, if not seconds. This makes spending on monitoring systems inefficient, and the cost of improving these real-time solutions often exceeds the cost associated with the threat itself. As a result, organizations that allocate extensive security resources to monitoring physical and cyber systems often fail to prevent crimes from occurring.

The reality is that having to explain what went wrong and how it happened is much more costly than allocating funds to preventing incidents before they occur. Yet most organizations focus solely on the cyber component with no real understanding of the broader function of identity management.

The focus must shift to prevention. It is also necessary to look at cybersecurity programs as a component of broader identity management for both logical and physical access.

Even the most robust cybersecurity program will not be completely effective without fully understanding the identity types within an organization and applying the concept of trust. PIAM solutions with predictive analysis capabilities allow organizations to gather data from a wide variety of IT, physical security and other systems. This data can then be cross-correlated to generate intelligence and detect anomalies associated with individual identities, which may indicate an insider threat. Shifting the focus to prevention enables security and management to stop threats before an incident occurs.

■ Back to TOC

Don Campbell (dcampbell@quantumsecure.com) is director of product management for Quantum Secure (www.quantumsecure.com). ✉

The largest contribution that IoT will make to security is in the proliferation of sensors that add to the data available for decision-making. The challenge for security practitioners will be to accept and even encourage the growth of these technologies, while harnessing the data and protecting both physical and network infrastructures.

A Standard Response to IoT's Security Challenges

Technical standards are essential to securing billions of connected devices

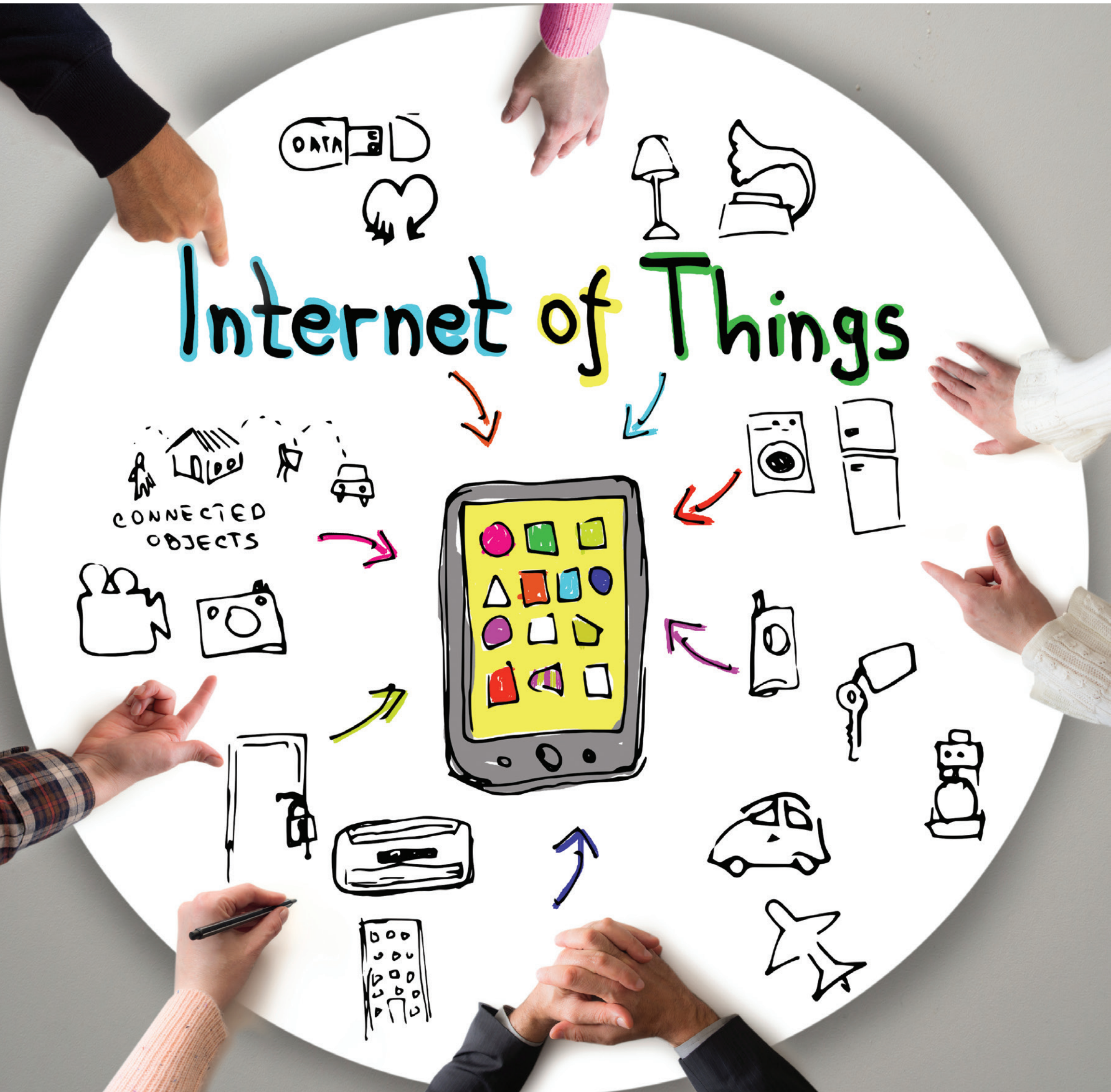
By Steve Van Till
Brivo Inc.

The Internet of Things (IoT) is causing an explosion in the number of connected devices. Many of these will be deployed on networks that are also a part of the security fabric of our facilities, our infrastructure, and – literally – our way of life. While they promise to make many positive contributions to our society and our personal experiences, they also open numerous new attack surfaces for cyber crime, identity theft, invasions of privacy, and even terrorism.

This threat has recently been dubbed a "denial of safety" attack, and it is expected to spread as facilities are increasingly equipped with IoT-like devices for both security and building automation. Accordingly, many in the technology community openly wonder whether this Pandora's Box can ever be closed. If it can, it will almost certainly require the adoption of standards that will help to contain the morass of special cases and one-off device profiles that are so burdensome and unsecure today. Without standards, it will only become worse, eventually giving way to the dystopian future of Ubisoft's *Watch Dogs* video game, in which an antihero can hack into physical infrastructure to "obtain and control information or destroy such devices completely."

Financial Drivers

The financial drivers behind IoT are large enough that the security industry cannot hope to escape its influence on the practice of protection. The economic impact of IoT between now and 2025 is estimated to be in the tens of trillions of dollars, according to forecasters as diverse as GE, Cisco, McKinsey and Gartner. That is a huge number, bigger than the impact of many of the recent technology trends that have already changed our lives dramatically. The sheer number of devices that will be added to the Internet is equally staggering: According to recent findings, that number was already at 3 billion as 2015 closed, and it will surge



to more than 20 billion by 2019. Connecting with all of these devices will be another 8 billion or so remote devices such as smartphones, tablets, watches, and even good old PCs, creating a "many to many" security problem of unprecedented magnitude.

Against this backdrop, there is a growing sense in the industry that IoT will play a significant role in physical security. The most obvious example is IoT in home automation, which usually leads with a "peace of mind" security message. These systems feature an expanding set of inexpensive wireless sensors and communications devices that are simpler and easier to install with each new generation of the technology. Even better, they interact effortlessly with all of our connected devices, from smartphones to wearables, so that we really do not have to think about having the right device with us in order to benefit from their services.

In the absence of standards, nothing can be secured, except one device at a time. That is neither scalable nor practical, and it would leave every network unmanageable at best and defenseless as worst.

It is less obvious – at least for now – how these or similar systems will cross over into commercial security, but the numbers say they will. According to *Business Intelligence*, out of the billions of IoT devices that will be connected to the Internet between now and 2019, only a surprisingly small 25 percent of that total will be installed in homes. That leaves three-fourths of them to be installed in enterprise (39 percent) and government or infrastructure (36 percent) settings. Many of these devices will be in service of physical security, broadly defined, including building automation, energy management, and presence monitoring, as well as traditional access control, surveillance, and alarm applications.

In fact, it is not difficult to argue that the electronic security industry has been using IoT since well before the term was coined and the current hype cycle catapulted the topic into daily fodder for both the professional and consumer media. The largest contribution that IoT will make to security is in the proliferation of sensors that add to the data available for decision-making. It is likely that some of this data will be generated by devices that were not originally deployed as part of the security enterprise. Many of them will have been installed or deployed by people outside the security practice. The challenge for security practitioners will be to accept and even encourage the growth of these technologies, while harnessing the data and protecting both physical and network infrastructures.

How Do Standards Fit into this World?

First, we need to accept the premise that, in the absence of standards, nothing can be secured, except one device at a time. That is neither scalable nor practical, and it would leave every network unmanageable at best and defenseless at worst. Standards have many benefits beyond basic interoperability. One of the most important is making devices conform to certain technical and behavioral patterns so that they can be treated as a class, not as individual instances. This is at the core of making them securable in any mass deployment.

Second, we need to recognize that there will not be just one standard for IoT devices. It would not be reasonable or practical to expect that all IoT devices could use a single standard, except at the most rudimentary levels (e.g., IPv6 addressing). IoT device capabilities and purposes are so widely divergent that there will need to be many standards to fit varying circumstances. They cannot just be shoe-horned into the same mold. A light bulb, a toothbrush and a security camera or sensor have very little in common, except that all may now be classified as IoT devices.

Third, we need to accept that the relevant standards for IoT devices – and even many security devices that fit within the IoT paradigm – will most likely be developed outside the security industry. On the one hand, this phenomenon is nothing new. The entire shift to IP represents a migration to a standard that came from outside the industry, specifically, the Internet Engineering Task Force (IETF). Similarly, the major video standards in every modern surveillance system originated from within the larger context of the Moving Pictures Expert Group (MPEG). On the other hand, the cyber risks presented by this new generation of connected devices have the potential to undermine the core mission of security if they are not properly managed. This observation has given rise to the point of view that "all security is now cybersecurity."

The sheer number of devices that will be added to the Internet is staggering: According to recent findings, that number was already at 3 billion as 2015 closed, and it will surge to more than 20 billion by 2019.

What Are Our Options?

The IoT landscape currently has a number of standards organizations and consortia vying for dominance. They each have their own distinct mission and, to some extent, have different target domains that they are aiming to standardize. The list that follows is not intended to be complete, but, rather, to present a sample of the most

prominent (and promising) standards as of this writing.

Open Interconnect Consortium

The Open Interconnect Consortium (OIC) was formed by Intel with the goal of connecting "the next 25 billion devices for the Internet of Things." The members of OIC are more than 50 of the biggest names in technology and consumer electronics. Its technical goal is to provide secure and reliable device discovery and connectivity across multiple OSs and platforms. OIC aims to deliver this by providing a "comprehensive communications framework to enable emerging applications in all key vertical markets." Their "IoTivity" project is an open source framework that provides tools to developers to help realize this vision.

All of OIC's specifications are online, with security being a central component of the model. The specifications in this area deal with trusted onboarding of devices, cryptography, protection of resources at rest and in transit, access control mechanisms, and device hardening.

All in all, OIC has produced a highly relevant set of standards for devices deployed in a physical security setting.

Google Weave

According to the Google Weave developer site, "Weave is a communications platform for IoT devices that enables device setup, phone-to-device-to-cloud communication, and user interaction from mobile devices and the web." The goal of the framework is to provide a common language that all devices in an ecosystem can understand. In the case of access control applications, for example, a door lock can have defined states or actions such as “lock” or “unlock” which can be issued by a variety of other devices, such as smartphones, or remotely via the Weave cloud.

Weave stands out among other contenders for IoT standards by virtue of having built-in security features, such as verified boot, data encryption, and the availability of automated security patches. Weave also has a robust set of methods for controlling what types of access permissions various devices and users have, an essential aspect of managing large numbers of devices in an enterprise setting.

The IoT and technology community at large are wrestling with the same cybersecurity issues that confront the electronic security industry today.

The Weave project also includes the Brillo OS, a stripped-down Android-based platform that is designed to run on the much smaller processor and memory footprints used by IoT devices. Assuming that this platform fits with a company’s development roadmap, it offers a significant bootstrapping opportunity for getting new IoT devices into production. Weave is also said to include libraries for other operating systems, so that the protocol and related discovery and security features can be available across heterogeneous environments.

Often confused with Nest Weave, Google Weave is intended to support connected devices broadly across the IoT space, not just in home automation applications. In this sense, it appears to be a more “industrial” set of standards that may be a better fit for security applications.

Allseen Alliance

The Allseen Alliance is a multi-industry consortium dedicated to enabling the interoperability of the billions of devices, services and apps that compose the Internet of Things. Its goal is to foster adoption of the AllJoyn protocol, which was originally created by Qualcomm and subsequently transferred to the Linux Foundation for ongoing maintenance and promotion. Primarily focused on WiFi applications, the protocol enables communications between peer devices, as in a home automation network. With more than 200 members, it is seen as a strong contender for standards success, and it saw its first significant crop of new products at this year’s Consumer Electronics Show, including light bulbs, security cameras, audio systems, and environmental systems.

Like the OIC, Allseen is pursuing an open source model for “implementing common services and interfaces that solve a specific use case, such as onboarding a new device for

the first time, sending notifications, and controlling a device." AllJoyn describes its security framework as "flexible and capable of supporting many mechanisms and trust models." However, it also says that, "AllJoyn security occurs at the application level; there is no trust at the device level." For an industry, like physical security, that is seeking standards that have trust and security as built-in features, this sounds a bit too open-ended to be very helpful. Leaving security to the application layer may work well enough for products that have mostly "siloed" work flows, but not for a heterogeneous collection of cooperating security and building automation devices.

Thread Group

Backed by the popular IoT device maker Nest, the approximately 100-member Thread Group ambitiously describes its one and only goal as, "to create the very best way to connect and control products in the home." As with the other IoT standards organizations, wireless communications between devices and to the cloud are major focal points of the initiative. Thread's use of a mesh communications network makes it a natural for home automation applications, but it could serve equally well in larger facilities, depending on distance and construction techniques.

Information security is one of the cornerstone services of the framework, which features "a smartphone-era authentication scheme and AES encryption to close security holes that exist in other wireless protocols." It intends to keep the user experience simple and familiar by using passphrases, yet providing a high level of security. How well this model extends to larger enterprise networks remains to be seen.

IEEE

The venerable IEEE has made an all-out effort to demonstrate its relevance to the IoT world and not lose out to newer standards organizations that could eclipse its central role in much of the standards-setting that has taken place in the electronics industry

over the past 50 years. To that end, IEEE has launched project P2413, "Standard for an Architectural Framework for the Internet of Things" and created a new website landing area for all things IoT (iot.ieee.org). With its hundreds of thousands of degreed engineers as individual members, IEEE has high visibility across every technology sector and is able to influence large numbers of new projects.

IEEE has also gone back through its existing body of standards and reclassified many of them (e.g., Ethernet) as "Internet of Things Related Standards" – helpful, at the nuts and bolts level, but not breaking new ground. It is also far less persuasive in many instances than the open source approach to standards that is used by the newer organizations in this space. Prescriptive specifications will always be needed, but open source code moves standards into real projects much more quickly.

One of the unique contributions IEEE has made will serve the interests of those who are still seeking a definition of IoT. The question is addressed – at length – in the May 2015 "Toward a Definition of the Internet of Things."

With respect to security, there is not much here that is immediately actionable, but it may turn out that IEEE's larger architectural project will have a longer-lasting impact on how we think of the IoT ecosystem as a whole.

The Rest of the Field

Without meaning to do a disservice to any organization active in this area, there are too many consortia and other industry groups to cover in anything less than a full-length book. Further complicating matters, new organizations come into existence almost monthly, and, unfortunately, disappear at nearly the same rate.

Some of these organizations are focused on very specific problems, such as data transport. The Oasis IoT group, for example, has been working on the telemetry transport protocols AMQP (Advanced Message Queuing Protocol) and MQTT (Message Queuing Telemetry Transport). While these protocols do not attempt or pretend to address the overall cybersecurity problem, they may find their way into security device applications and would, therefore, need to be secured within the larger context of systems integration or network security.

The IETF is also very relevant to the ongoing development of IoT standards, as with the "IPv6 over Low Power WPAN" standard that is being implemented to extend IP networking to very low-power devices. Again, securing a network using this protocol presents many of the same challenges as securing the IP networks in use today, and the standard does not speak to the layer of the problem.

The SIA Cloud, Mobility and IoT Subcommittee

The SIA Standards Committee formed the Cloud, Mobility and IoT Subcommittee to examine cybersecurity and many other issues related to the adoption of IoT in the physical security sector. The purpose of the group is to develop, discover, influence, and provide education around standards relevant to the challenges of combining these three technologies in security applications. The rationale for doing so includes the following principles:

- IoT devices will produce data that is useful to the physical security mission.
- Security systems can harvest this value only if the industry knows how to build secure IoT deployments that interoperate with security management tools.
- IoT devices will use communications standards originating outside the security industry; namely, from IoT vendors, consortia and large Silicon Valley players.
- IoT can enhance physical security, but only if cybersecurity risks are properly mitigated.

The SIA Standards Committee has an advisory and educational role in addition to its standards-making role. Therefore, given the significance of IoT and its dependence on technical standards, the group will continue to drive answers to the question of standards for IoT in security.

Where to from Here?

At this writing, there is nothing close to a set of broad answers for how IoT can be secured, although it remains clear that technical standards are a foundational part of the equation. The IoT and technology community at large are wrestling with the same cybersecurity issues that confront the electronic security industry today. What is clear is that we will not solve this problem within the security industry alone, and that some set of IoT standards will provide the basis for enough uniformity that we are not playing an impossible game of Whac-A-Mole. ■ Back to TOC

Steve Van Till (steve.vantill@brivo.com) is president and CEO of Brivo Inc. (www.brivo.com). He serves as chairman of the SIA Standards Committee. ✉

Threats to data security happen when hackers target the weakest link in the chain, and without the appropriate technology and policies, the risk that the security system will be that weakest link is real.

Don’t Be the Weakest Link

Security, IT Departments Must Work Together to Reduce Vulnerabilities

By Stuart Rawling
Pelco by Schneider Electric

The physical security industry has generally not received a lot of attention when it comes to cybersecurity issues, breaches and threats to data. However, with the shift from analog to IP devices, and with a more converged network of devices, many organizations have found themselves face-to-face with the issue of data security as it applies to physical security equipment. How can they best formulate robust policies and strategies to protect against network threats?

Think back to the 2001 film “Ocean’s Eleven,” in which a team of thieves and con men carried out an elaborate scheme to rob three Las Vegas casinos. As part of the heist, a video surveillance system was hacked and the feed was replaced in order to mislead the owner of the casinos.

While this, of course, was just a movie, the plot point demonstrates the dangers that come with having elevated levels of connectivity without proper security protocols.

Today’s technology marketplace is full of connected devices – the smart home, apps that allow security managers to view video from various locations, remote access control devices and more. The thinking has shifted from the *possibility* of attack to the *probability* of one or more occurring. Bad actors are attempting to circumvent security on network devices for a variety of purposes, ranging from using the devices deployed in a physical security installation in an attack against another Internet-connected device or service, or degrading and breaching the security system itself, as was the case in the movie. As networks converge, it is unfortunately inevitable that more attempts to circumvent physical security systems will occur.

There are ways to protect IT networks, however, including identifying possible weaknesses in technology and policies, learning from colleagues in the enterprise IT realm, and following industry standardization of products.

Technology and Policies

There are two elements to ensuring the safety of corporate data: the right technology and the right policies.

Some connected security technologies have been found to have vulnerabilities and to adhere to less-than-ideal security practices. The good news is that manufacturers are working to fix these problems. It is imperative to address possible concerns with data security before products are released to the public. Additionally, it is important for manufacturers to educate end users how to protect themselves from breaches – for example, by changing the default usernames and passwords on cameras once they are installed.

Second – and arguably more important – companies and

organizations utilizing physical security equipment must have cybersecurity policies in place that outline proper procedures for handling sensitive information and data. Training employees in security principles by establishing best practices, such as requiring strong passwords and establishing appropriate Internet use guidelines, is critical. In addition, users should ensure that they do the following:

- Update security software
- Provide a firewall for Internet connections
- Create a plan for the use of mobile devices
- Back up important data using secure means
- Secure WiFi networks
- Require employees to use strong passwords and authentication
- Implement policies for controlling access to equipment
- Train employees to watch for social engineering tactics such as:
    - Pretexting
    - Phishing
    - Baiting

In today's ever-evolving market, it is not just about how manufacturers can protect end users, but also about how end users can best utilize the security technology that manufacturers provide.

> *There are two elements to ensuring the safety of corporate data: the right technology and the right policies.*

Learning from the Enterprise IT Model

The physical security industry can learn a significant amount from the enterprise IT sector. When IT first began seeing a shift to a more secure environment, many businesses were on their own network – the printer network, if you will – and hacks were performed on a smaller scale. At that time, there were not many instances of "attacks" being malicious. Fast forward to today's connectivity, and the threat of harmful IT breaches has increased at an alarming rate.

In the health care sector, security experts dubbed 2015 as the year of the health care hack. In January 2015, 11 million Premera Blue Cross customers were affected by a large-scale breach. This was followed by a breach at Anthem that affected nearly 80 million current and former customers in February. A UCLA Health System breach in July affected 4.5 million people, and in September, Excellus BlueCross BlueShield in upstate New York had the records of as many as 10 million people exposed by hackers. And this is just a sampling of incidents. In total last year, there were more than 112 million health records breached in 253 incidents, according to the Department of Health and Human Services.

Then, early this year, hackers held the records of patients at Hollywood Presbyterian Medical Center hostage until a ransom was paid – 40 Bitcoins (equivalent to $17,000).

It is important for manufacturers to educate end users on how to protect themselves from breaches – for example, by changing the default usernames and passwords on cameras once they are installed.

The health care industry is particularly susceptible to these attacks because the shift to electronic medical records has increased the need for access to previously non-electronic data, as well as because of the sheer amount of information collected, including Social Security numbers, credit card numbers and sensitive medical information. The industry is learning the hard way that investing in a stronger cybersecurity plan to prevent and combat breaches is crucial to the overall health of the organization.

Recent breaches have prompted IT departments across a wide variety of markets to take a firmer stance on how information is shared, how networks are built and how devices can be used on a company's property. The connected enterprise contains a lot of crossover, and large corporations have to adhere

to strict IT policies on how devices within these networks can be used. Employees must be educated on proper usage in order to protect the data being shared between devices.

Merging Physical and IT Security

The physical security industry has long developed cutting-edge technology that pushes the boundaries of innovation, but it has not always fully addressed the details of IT vulnerabilities. As more manufacturers develop wireless and cloud-based systems, special attention must be paid to the security of the devices. This means that the previously separate IT security and physical security departments must collaborate to ensure the safety of data across the enterprise organization and beyond.

Today's security manager must be mobile, and this requires access to data from anywhere at any time. App development for video management systems is booming, allowing the flexibility to access critical data through web-based platforms. But it is imperative that security leaders work closely with IT departments to discuss possible weaknesses in access points and communicate effectively on how to overcome these issues. Security managers must be agile and in tune with this notion of protecting critical data and access points, which reaches far beyond traditional physical security borders.

Threats to data security happen when hackers target the weakest link in the chain, and without the appropriate technology and policies, the risk that the security system will be that weakest link is real. For example, if a wireless camera is broadcasting an entry point to a building and its feed is not secured, attackers could gain access not only to the video feed, which they could use to determine who enters and exits a facility and at what time, but also to the corporate network itself. The possibility that security equipment could be used as an entrance to the greater enterprise network is a cruel irony that poses a significant threat to any organization.

Standardizing Video Surveillance Data Collection

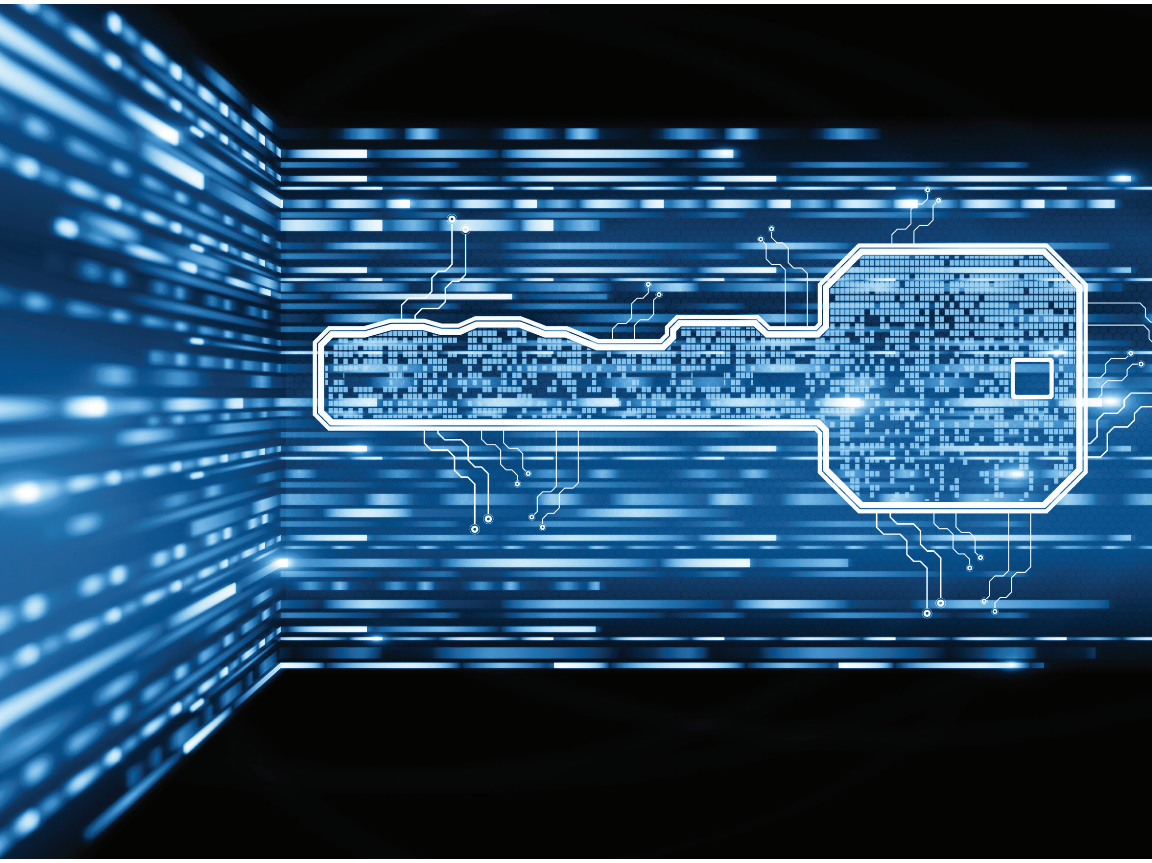
Several alliances have been formed to work on automation and communication protocols to help organizations prepare for the increase in IoT devices "talking" to one another. This standardization of communication protocols is critical to the success of business in an IoT world.

IoT will require physical and IT security manufacturers to work together to establish baseline standards that allow physical security systems to work with devices outside the industry, similar to how ONVIF worked across manufacturers to elevate the usability of video surveillance products. ONVIF, in fact, recently published the Profile Q standard to provide "out-of-the-box interoperab-ility" for IP devices. Similarly, both the PSA Security Network and the Security Industry Association have created advisory boards focused on addressing IT security issues in the physical security space. This demonstrates that the industry is taking the steps necessary to address these concerns and implement the proper procedures by which to regulate these matters.

Encryption and cryptographic methodologies, such as security certificates and electronic data signatures or watermarking, are critical tools manufacturers use to ensure that the data being collected over a network is kept secure. Deploying these technologies along with a strong cybersecurity policy is an important first step to ensuring protection of the system, its data and the network as a whole.

> *The possibility that security equipment could be used as an entrance to the greater enterprise network is a cruel irony that poses a significant threat to any organization.*

There is no need for manufacturers to develop new cryptographic technologies; the cryptography technology available today is mature, robust and thoroughly tested. At the center of cryptography is some very hard math, and there are researchers around the world validating and probing the technology on a continuous basis. It is not a good practice to try to come up with something new cryptographically and keep it a secret, as security through



obscurity is not security at all. It is a best practice for manufacturers to use established and tested methodologies, and, most important, to describe the methodologies that are used.

The Future of Connectivity

Consumers of modern technology have certain expectations, such as being able to use mobile phones or devices in a connected home quickly and simply. Security and ease of use are often in conflict, though. The easier it is to use something, in many cases, the less secure it becomes. It is necessary, then, to find a middle ground for protecting valuable information while maintaining convenience by bringing together key players from the physical security and IT sectors to standardize the relationship between security and IoT functionality. Without that cooperation, organizations will face unacceptable risks to their data.

■ Back to TOC

Stuart Rawling (stuart.rawling@schneider-electric.com) is director of business development for Pelco by Schneider Electric (www.pelco.com). ✉

While security systems can be effective at mitigating risk, they also represent additional points of vulnerability that must be hardened if the net effect is to be an improvement in security.

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.

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

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.

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.

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.

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

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. ■

Back to TOC

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.

A CEO's Guide to Cybersecurity

Identifying and addressing vulnerabilities must be a priority

By Hans Holmer
Intelligent Decisions

Cybersecurity responds to leadership priorities just as finances and human resources do. Computers and networks come with flaws and vulnerabilities, as with all other aspects of a business, and these vulnerabilities enable hackers to achieve their goals. The CEO mitigates risk, regardless of domain, by exhibiting leadership and delegating day-to-day responsibility for given areas to specific individuals who are held accountable for strategies and results based on the expectations of the CEO and board of directors. Within cybersecurity, the chief information security officer (CISO) is responsible for ensuring that the CEO's priorities are implemented and advises the CEO on the strengths and vulnerabilities of current policies. A good CISO is a key player in maintaining internal network security and advising designers and engineers on the security of products and systems, as well.

Security Begins at the Top

Security has typically been an afterthought in the cyber technology market and, although the curve is bending slightly in mass market systems, it will continue to lag behind customer needs. While mass market operating systems are doing better with features such as automatic updates, industrial control systems (ICS) and the Internet of Things (IoT) will likely continue to lag, both because of the large installed base and a general reluctance to making security a key driver compared to essential functionality.

As a consequence of this continued vulnerability to hackers, it is imperative that operators of ICS and IoT systems design and operate them with critical defenses built in from the start. The essential best practices outlined below are aligned with best security practices in conventional computer networks, such as those recommended by the SANS Institute and the National Institute of Standards and Technology (NIST). They are based on the premise that the best way to defeat a hacker is to close the vulnerabilities that hackers exploit to gain entry.

Assign Responsibility

The first critical step an organization should take is to appoint a senior security officer who primarily acts as the advocate for and assessor of the critical data and process security within the organization. Critical data and processes can include financial, personnel, industrial process, video, lock systems, and whatever is critical to the continued existence of the organization. In most businesses, the senior security officer is the CISO, and this person's responsibility should include processes and other significant technologies that use information

technology. The CISO also needs to ensure that the organization has the ability to detect when it has been hacked, something that, today, is discovered by a third party in almost all cases.

Identify Critical Data and Processes

The first project for a new CISO is to determine what data streams and processes, both internal and external, are critical to the business. Companies that make or integrate security cameras might want to ensure the integrity of their products, of their financial and personnel records, and of any external dependencies such as servers and operating systems sourced from other vendors. Technology is truly a poly-culture that is mutually interdependent, and a failure in one system can have widespread deleterious effects. No computer is an island.

Very little physical security equipment does not have a cyber aspect, which promises better security management but is also associated with an increased number of potential vulnerabilities, both to subversion and to denial of service.

Initiate a Culture of Security

Having figured out the products, processes and data that are critical, the CISO needs to start building a security culture within the organization. This culture will encompass all aspects of equipment design and building, network architectures, customer interaction and staff awareness. The CISO should also designate "thought leaders" for the corporate centers of gravity where security awareness is particularly critical. C-level executives are important to annunciating and demonstrating that security is a critical value for the corporation.

Inventory the Network

There are a number of critical areas that the CISO can assess to judge the maturity of an organization's security posture. These are all basic, but adherence to these security protocols can help prevent almost all of the intrusions directed at networks and systems. The first one is whether the organization is able to identify all systems within its own network and to define a perimeter between inside and outside. Modern networks have become very fluid, much like modern battlefields, and they frequently include personally-owned devices such as mobile phones and computers. This may not be avoidable, but CISOs and CIOs can ensure that especially important data and processes stay within specific network enclaves and can build the network for security as well as reliability. As the network is redesigned and rebuilt, they must not forget to produce and maintain adequate documentation for the network, both as-designed and as-built. This makes it possible for future engineers to understand and improve the design quickly and securely.

Update the Network

The second major criterion is whether all devices on the network have the latest software version and patches. All hardware and software needs to be a version that remains supported by the manufacturer, and the CIO should have a process for ensuring that operating systems and software are patched in a timely fashion. A very high percentage of the patches made available by manufacturers fix newly discovered vulnerabilities in systems and are exploited by hackers within a week or two after being made public. Although some vulnerabilities continue to be exploited for years after patches are issued, many are time-sensitive. Failure to install patches is a critical component of breaches by hackers.

Zero-Days

Zero-day attacks are intrusions that take advantage of vulnerabilities that have been known to the manufacturer for zero days. Once a manufacturer is notified of a new vulnerability, it generally tries to keep the vulnerability secret until a patch can be released, but once the patch is made available, it does not take long for hackers to reverse engineer the fix to discover the original vulnerability and write an exploit. The shorter the interval between the disclosure of the vulnerability and the installation of the patch, the better. Unfortunately, new patches may create instabilities in dependent systems and CIOs are

reluctant to introduce changes in systems that are working. This is a hard-to-win position for the CIO, and one of the jobs of the CISO is to provide cover for the CIO to increase the speed of the patch cycle in order to shorten the exposure window, even if this might cause downtime.

Improve Access Control

The final key metric that needs to be assessed is how closely employees' access control boundaries meet their actual needs. Many highly efficient organizations assume that fewer administrators with more access equals greater efficiency, but they do not consider the increased risk that comes with a small number of people having very broad access. Staff members ideally should have no more access than they need to do their jobs, and they generally should not have any administrative access. Similarly, administrators should not be able to answer their email with administrative privileges. While this may increase salary costs, it reduces a disgruntled employee's ability to do harm to a network. It also prevents a hacker from gaining broad access to a network by getting access to one employee's or administrator's login credentials. This is another area where the CISO provides cover for the CIO to ask for more staff to enable better separation of duties and reduce long-term risk to the company's data and processes.

The best way to defeat a hacker is to close the vulnerabilities that hackers exploit to gain entry.

Password Hygiene

Having tightened the access of administrators and users alike, the CISO needs to ensure that the organization requires and enforces good password hygiene. Every year, there are reviews of the most common passwords found after hacks, and, invariably, passwords like "12345678" or "qwerty" come out on top. Each complex password may only be used for one system and must be at least 12 characters long, using each of the four character types on the keyboard – lowercase letters, uppercase letters, numbers and special characters – in a manner that does not suggest a word or phrase. Similarly, the CISO must ensure that all stored passwords are hashed to prevent prediction algorithms from solving them. The CISO should also ensure that all default passwords on devices are changed as soon as they are deployed. For users or administrators who need to have multiple accounts and passwords, password managers are an excellent tool for organizing them.

Security Metrics

It is hard, if not impossible, to generate meaningful measures of security. However, it is possible to measure and compare some critical metrics regularly. These include the number of new devices found on the network on a weekly basis, the percentage of devices that are fully patched, changes in privileged user accounts compared to changes in personnel, and other fundamentals. Many appliances generate metrics that are perfectly true but are of no use in assessing the actual security posture, so it is critical to focus on basic metrics that measure the effectiveness of security measures rather than the scans of hackers.

Regular collection of security metrics makes it possible to spot trends and identify significant patterns. It also provides data about how good an organization is at doing basic security processes, which will not be better than its ability to do sophisticated security processes. Companies that provide security risk benchmarking-as-a-service will measure which vulnerabilities they can detect from outside the network.

Hackers know that the patch cycle in their targets is long enough that it only requires a limited amount of ingenuity and persistence to get in. As long as system owners persist in making security a secondary consideration this will not change.

Vulnerability Discovery

The above principles hold true for conventional computer networks, physical security networks, and all other connected devices. They are critical for both manufacturers and their products. In addition to sponsoring security advocates within the design and manufacturing chain, companies need to create simple and secure models for patching their products to enhance capabilities and security. While some of the security vulnerabilities will be discovered internally, such as the implementation of backdoors for testing or convenience, companies should create a responsible disclosure reward system in which hackers are paid for disclosing vulnerabilities in a way that gives the company time to issue patches before the vulnerability is widely known.

Security in Design Choices

At the same time, integrators of equipment from multiple vendors need to increase awareness of supplier security postures and work to define maturity models. Very little physical security equipment does not have a cyber aspect, which promises better security management but is also associated with an increased number of potential vulnerabilities, both to subversion and to denial of service. Various technologies offer different advantages and vulnerabilities in communications links and failure modes. It is critical to consider the entirety of the infrastructure, as vulnerabilities frequently arise in the seams between different systems. A holistic approach that fuses all aspects of the network, including physical and logical aspects, and also prevents

counterfeiting of hardware and preserves the integrity of software, is critical.

Wireless Communications

Wireless connections offer freedom from running a lot of cables, saving time and money. At the same time, though, they are difficult to implement securely and are vulnerable to jamming, which may cause equipment or connectivity failure. Equipment failure may cause awareness gaps, and this requires designers to plan whether equipment should fail "open" or "closed." A door that does not open when human safety requires it can cause deaths. Systems closing when they should be open also is not good. In either case, failure modes need to be part of the design criteria.

Cryptography

Some engineers may say that they can design and build a cryptographically-secured communications protocol. They are wrong. Many people have tried to do it with, for example, satellite TV, encrypted movies and music, and "smart" electric meters. They all used home-brewed cryptography and they all failed to withstand even modest efforts to penetrate them. Good cryptography relies on well understood, thoroughly tested protocols, such as those approved and sponsored by NIST and used on the Internet. After the installation of good crypto algorithms, attention must be paid to key length and management. History shows that cryptography typically fails because of user mistakes, not algorithm vulnerabilities, so companies must ensure that the end-to-end application is secure by having it reviewed by a capable third party.

Multi-Purpose Computers are Less Secure

Computers are good general purpose machines that can do many things simultaneously – but they rarely can do many things securely. The more things running on one machine, the higher the likelihood of interference or vulnerabilities between software packages. It is common to see ICS interfaces running on machines that also allow corporate and external email. This makes the ICS software vulnerable to email spear phishing designed to get users to click on embedded malware or links. Spear phishing is one of the most common attack vectors, and attackers are consistently ahead of antivirus defenses and defensive perimeter machines. It is much more secure to run ICS systems separately from the corporate LAN. Similarly, since hackers know that senior personnel have extensive access, they often try to spear phish them directly – which is known as whaling – forcing CEOs and others to be extra aware of the potential threats that can come from clicking on links within unusual emails.

Silver Bullets

Many companies would like to sell customers a silver bullet that protects them from all digital threats. This is an alluring proposal, but it is not one that bears out in reality. 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. For more details, search for "CIS critical security controls" on the Internet.

Supply Chain

The supply chain includes technology with known and unknown flaws. Companies should never assume that any part of the supply chain delivers flawless products. Rather, they must assume that every part of the supply chain requires continuous mitigation of whatever flaws are known, and must use an architecture that is based on the assumption that vulnerabilities are present.

A company that makes a product that can receive updates should consider using cryptography to secure the updates, all the way from the software development center to the customer's device, after exhaustive testing. Not only does this make it harder for hackers to subvert the functionality of the product, it can also protect the intellectual property that is contained in the device and the update, and ultimately protect the company's reputation. Again, the capability and process for secure firmware and updates usually needs to be designed in from the beginning.

Insider Threats

There will always be some insider threats, whether deliberate or accidental, malicious or careless. Companies must, then, design, build and manage their networks with that assumption in mind, building in safeguards that protect the confidentiality, integrity and availability of critical data and processes. They will not be able to detect insider threats in advance – after

all, anybody who has one password for multiple systems or uses weak passwords is a risk – and many insider threats will never be detected. Insider threats that are detected are generally found by third parties, such as auditors. This reflects poor efforts at detecting insider threats in the act more than it does the quality of audits, as insiders generally are not caught quickly. The most likely avenue for detecting insider threats is to monitor how data moves within the network and to compare that to how it should move.

Hackers

There are hackers out there who cannot be stopped, but that is not the same as saying that no hackers can be stopped. The vast majority of hackers exploit vulnerabilities for which there are patches and mitigations. They know that the patch cycle in their targets is long enough that it only requires a limited amount of ingenuity and persistence to get in. As long as system owners persist in making security a secondary consideration, this will not change. As with cryptography, the technology is sound but the implementation is weak. And that is where the C-Suite can make a difference.

No Defense is Perfect

Odds are that some attackers will get inside the network. The systems need to be able to detect abnormal behaviors by users or systems before the hackers get to the critical data or processes. Good auditing of systems, looking for abnormalities in behaviors, volume and content, is critical to understanding what is happening within the network. Following the discovery of abnormalities, the defense team needs to implement a predetermined plan to defeat the intrusion before it succeeds. No amount of planning will predict every possible attack, but a practiced set of responders who know each other well can be very effective against most hackers.

The Nutshell

The key to cybersecurity is managing vulnerabilities. Companies that focus on minimizing vulnerabilities and quickly detecting intrusions will be the most secure.

■ Back to TOC

Hans Holmer (hholmer1@gmail.com) is the senior cyber strategist in the Technical Intelligence Center at Intelligent Decisions (www.intelligent.net). He is a member of the SIA Cybersecurity Advisory Board. ✉

As organizations across the globe reap the benefits of the connected world, new ways must be found to enhance the security of IoT devices from both a cybersecurity and physical security perspective.

Tackling the Complexities of the Connected World

Enterprise security must be a team effort

By Herb Kelsey
Guardtime

Cybersecurity trends and risks are top of mind for nearly every business leader today, and these executives are turning to security professionals within their organizations to keep pace with IT security risks while also helping secure people, critical data and physical assets. As the world becomes more connected, and risks grow more sophisticated, this is a complex undertaking for even a seasoned executive, IT expert or security professional.

Cybersecurity is a difficult and serious endeavor that forces IT leaders to find balance in managing the security of the computing capabilities that connect and enrich lives. Today's security leaders are at the crossroads of ensuring the safety and security of physical assets and keeping critical data safe from outside threats. For enterprise IT teams to know quickly when their environments have been tampered with, they must align operational technology (OT) and IT security priorities. This strategic approach also allows for a discussion about ways to modernize security to protect legacy infrastructure systems.

Emerging network trends related to reducing the time it takes to detect tamper and the growing demand for secure mobile computing provide a call to action for enterprises seeking to transform the nature of risk assessment in an IT-driven environment.

Billions and Billions of Devices

The Internet of Things (IoT) takes shape from connecting any device with an on-off switch – smartphones, coffeemakers, automobiles, wearables, lamps, appliances, not to mention critical infrastructure, such as the energy grid or public transportation systems – to the network and to each other so that data can be shared. This connectivity enables systems to operate more efficiently, making lives a little easier. It is a co-existing relationship between people and things for the betterment of the human condition. And it is growing – quickly.

Many reliable sources are studying the growth of IoT as the world becomes hyper-connected, and there is no doubt that adoption is proliferating: Research firm IDC says that the global IoT market will grow to $1.7 trillion by the year 2020; the World Economic Forum indicates that the number of connected devices is projected to grow from 22.9 billion this year to 50.1 billion by 2020; and IC Insights predicts that new IoT connections will grow from approximately 1.7 billion now to nearly 3.1 billion in 2019. The statistics are astounding, to say the least, and with this type of global connectivity, a growing number of security challenges will emerge.

According to research conducted by Gartner, by 2020, IoT will comprise approximately 21 billion devices. Gartner also reports that, “IT leaders will have to accommodate the differences in technologies across those areas and develop a multifaceted technology approach to IoT risk and security.” Additionally, Cisco’s Visual Networking Index (Cisco VNI) indicates that IoT devices will dominate the network by 2018, meaning that machines will communicate over the Internet more than humans. This growth leads to vulnerabilities. The more everyday objects are connected and

communicate virtually, the more we open the door to security threats.

IoT devices will dominate the network by 2018, meaning that machines will communicate over the Internet more than humans. This growth leads to vulnerabilities. The more everyday objects are connected and communicate virtually, the more we open the door to security threats.

Protecting IoT Devices in the Enterprise

Since this technology is becoming more and more ingrained into daily lives, at the very basic level, users need to be able to trust that IoT devices and the data being transmitted are secure from vulnerabilities. If entry points are not protected, the risks of cyber attacks and data acquisition by theft are very real. Further complicating security is the deployment of IoT devices that automatically connect to other IP-enabled technologies, increasing the likelihood that these products will transmit data into unsecure environments.

With more data being shared, the possibility of security breaches increases as cyber criminals see value in hacking into IoT devices, resulting in vast amounts of information from many systems being compromised. In February, hackers seized control of Hollywood Presbyterian Medical

Center's computer systems and only gave back access after a 40 Bitcoin (equivalent to $17,000) ransom was paid. According to Forbes, data breaches in health care alone compromised more than 112 million records in 2015.

Part of this stems from the fact that all devices trust each other, and share data back and forth without verifying source credibility. Should sensitive data get breached and fall into the wrong hands, public safety – and, in essence, security – could be compromised. Some IT and security experts propose that professional and ethical standards be established and followed so that everyone shares the responsibility of security as it relates to IoT.

With this type of global connectivity, a growing number of security challenges will be presented.

It is impossible to size, much less identify, all of the vulnerabilities associated with IoT because it is still unfolding, and to date, there are no easy, one-size-fits-all solutions. As organizations across the globe reap the benefits of the connected world, new ways must be found to enhance the security of IoT devices from both a cybersecurity and physical security perspective.

Blending Physical and IT Security

Cybersecurity risks have expanded, networks are growing, hackers have gotten smarter, and resources are typically limited by budget constraints.

Privacy is also a critical topic. How can organizations meet privacy and security standards in this ever-evolving connected world? IT leaders have to work harder, and smarter, than ever to develop stronger security infrastructures, policies and strategies within their organizations to accommodate these changes. The overarching goal is not only to ensure uptime and performance of the network, but also to protect assets and corporate data. Collaboration across departments can help address how information and access to data should be controlled, as well as who should be responsible for the protection of that information.

This leads to the concept of an overarching approach to security, with cybersecurity and physical security teams coming together to ensure the safety and protection of people, assets and information using physical barriers and technology in an IoT-connected world. Over the years, a blurring of divisions has occurred. Gone are the days of siloed IT and security operations. Navigating a collaborative relationship between information security officers and physical security directors is critical to maintaining a high level of protection. CIOs and CISOs should also engage boards of directors in discussions of cybersecurity and risk evaluation, and build a collaborative framework within an organization's executive leadership to address information risk. This includes incorporating technology-driven solutions and strategies to best address threats within the secure enterprise, reduce the time it takes to detect threats, and build effective response plans.

The convergence of the cybersecurity and physical security worlds has been discussed for several years, and today many leaders believe it is long overdue. New threats appear every day that make us question data protection levels, and new innovations and processes are enabling the complete mobilization of the secure data center without limiting functionality. But without combining these new capabilities with complete protection, data can easily be compromised. A dialogue between IT and physical security leaders is necessary to help business leaders gain greater knowledge of how to work together to ensure data protection.

Establishing Standards and Procedures

Cooperation between multiple departments within an organization is only the beginning. Multiple studies on breaches and infrastructure attacks show that most can be deflected by using simple, well-known security measures. Industry leaders must be able to communicate with multiple departments to identify vulnerabilities and work collaboratively to address these challenges. Enterprise IT teams must converge to understand when their environments have been tampered with to quickly address breaches.

Are protocols needed beyond typical cyber safety protections? Is more collaboration needed between enterprise security teams? Here are three ways to further bridge the gap:

- Make security a priority by building it directly into the network. Include multi-layer IT and security protocols for all sensors, devices, applications, data and firmware to create multiple layers of defense with a focus on the integrity of the system assets.
- Use analytics to determine network operation trends. This data provides detailed insight that enables users to see suspicious trends emerging, providing the ability to alert network administrators when risks are identified.
- Be proactive by building a comprehensive security strategy that is customized to fit an enterprise's specific needs. With the push for connectivity and mobility, security can be overlooked. Therefore, it is critical that organizations empower employees to identify potential vulnerabilities. This will go a long way toward managing risks.

Multiple studies on breaches and attacks on infrastructure show that most can be deflected by using simple, well-known security measures.

The continued combination of the cybersecurity and physical security worlds will help build a holistic security strategy for connected organizations. The secure global enterprise can only be achieved when physical and information security integrate to mitigate emerging and complex cyber threats in a hyper-connected world.

Discussions about cybersecurity threats and strategies for mitigating those threats must be ongoing. IT security leaders must stay informed on the latest threats and should seek out opportunities to attend events dedicated to IT and physical security technology. These events should be used to network with leading industry voices, influencers and thought leaders in order to share knowledge that can help ensure today's and tomorrow's secure enterprise. They should become familiar with the latest technology trends and ask questions specific to their organization's challenges. And, most important, they should exchange information with their peers, leading solutions vendors, security practitioners, and industry thought leaders to grow their network and contribute to industry progress. By working in collaboration, organizations across the globe can effectively protect corporate data and networks and ensure long-term business viability.

■ Back to TOC

Herb Kelsey (hkelsey@guardtime.com) is the chief architect at Guardtime (www.guardtime.com). He is a keynote speaker at the 2016 Connected Security Expo at ISC West. ✉

For security vendors in the traditional physical security space, it is clear that there is a significant risk that their products and services will be attacked, and that the consequences could be very detrimental, both to customers and to the company's bottom line. So what can be done?

The Importance of Practicing 'Due Care' in Cybersecurity

Taking appropriate precautions can prevent security equipment from being a cyber vulnerability

By Dave Cullinane
TruSTAR

Cybersecurity and physical security are becoming more and more connected. Everything from the cars people drive to the heating systems that warm their houses to the planes they fly in are increasingly controlled by interconnected computers. And, as a result, they are subject to attack.

Target sustained a major cyber breach through its HVAC vendor. That breach resulted in the firing of the CEO. Cyber-physical security, as a result, is on the minds of every C-level executive and board of directors member, from major corporations to small businesses. This means that security equipment companies have a responsibility to make sure that the systems that are used to secure those businesses are not the vulnerability that enables a cyber attack to be successful.

Supply chain security is also an increasing concern today. An employee of a small company (fewer than 200 employees) that builds customized high-tech components for major corporations recently related that his employer had been hit with a ransomware attack. All of their production systems had been encrypted, and the attackers demanded money in exchange for the decryption key. This company did not have a security function.

Small and midsize businesses (SMBs) are the core of America's business growth, yet they are the least likely to have the level of security expertise needed today – particularly cybersecurity expertise. Their focus is entirely on their core business. The principles of security are the same, though. Cyber is just a specific type of security expertise.

Is a given company at risk of a ransomware attack? Is there someone somewhere in the world that might like to hurt the business by hitting it with a denial-of-service attack? Does it or its employees use the Internet and receive email? Does everyone have a smart phone? Do they work at home? Does it work with companies that are likely to be attack targets? If it is supplying products to major corporations, might those corporations be concerned about the products being the source of an intrusion? For most companies, all of the above is probably true. It is part of being a company in the Information Age.

Security equipment companies have a responsibility to make sure that the systems that are used to secure those businesses are not the vulnerability that enables a cyber attack to be successful.

So how real is the threat to a company's products? It is very, very real.

- In 2015, 100,000 new pieces of malware were created every day. That is roughly one per second. Can a company's anti-virus product keep up with that?
- There are 80 to 90 million or more cybersecurity events per year, with close to 400 new threats every minute. Up to 70 percent of attacks go undetected.

- Someone who does not like an organization can rent a denial-of-service attack online for $10-$20 that is capable of taking all but the most sophisticated networks down.
- 60 percent of attacks are directed at SMBs.
- Symantec reports that, "Cyberattackers are leapfrogging defenses in ways companies lack the insight to anticipate."
- As Dan Geer pointed out, "The CISO has to find and fix every vulnerability. The adversary only has to find one he/she can exploit."
- Many hackers create attacks, then turn them into kits that they can sell, allowing them to make millions with virtually no risk. So there are lots of unsophisticated attackers using highly sophisticated attacks.
- Other hackers take the original attack kit and modify it, making new versions that are immune to the protections that were created to stop the original.
- Attacks spread rapidly. The *Verizon 2015 Data Breach Investigations Report* found that attacks can reach dozens, even hundreds, of other companies within 24 hours.
- And finally "The cyber insurance market will dramatically disrupt businesses in the next 12 months. Insurance companies will refuse to pay out for the increasing

breaches that are caused by ineffective security practices, while premiums and payouts will become more aligned with the actual cost of a breach. The requirements for cyber insurance will become as significant as regulatory requirements, impacting on businesses' existing security programs."

– Carl Leonard,
Principal Security Analyst,
Forcepoint Security Labs

There are 80 to 90 million or more cybersecurity events per year, with close to 400 new threats every minute. Up to 70 percent of attacks go undetected.

Cloud computing, particularly the concept of security-as-a-service, has had a big impact on the security industry. But manufacturers and service providers face the challenge of ensuring that their equipment and services are secure. Cybersecurity for video is also a very significant concern. Digital video has to be demonstrably free from tampering to meet most customers' needs. The most efficient storage for digital media, by far, is in the cloud, but how do you ensure the integrity of video data in the cloud? Encrypting it in storage is a big help, but how do you make sure it is not tampered with in transit or while it is being used by applications? There are products today that allow applications to use encrypted data, so the cleartext

data is never exposed. Who controls the encryption keys is another issue. Edward Snowden has made the trusted third party model obsolete. The same product that allows applications to use encrypted data also allows the creator of the application to control the keys.

Almost all online security applications use a browser. But browser security is a major concern, particularly when a customer is using a browser that has been to unsecure places. There are companies today, though, that provide extremely secure browsers that operate as simply and easily as what customers are used to while protecting them from being victimized and protecting security equipment and service providers from being accused of causing a problem.

The vast majority of companies find out they have been breached when someone else tells them, usually a customer or partner.

For security vendors in the traditional physical security space, it is clear that there is a significant risk that their products and services will be attacked, and that the consequences could be very detrimental, both to customers and to the company's bottom line. So what can be done? One must assess the company's security posture:

- What information and data is received, transmitted or stored as "cyber data" (on computers, networks, databases, etc.)
- How is that data protected from cyber attack? Are anti-virus products, data integrity tools, etc. used? Are development and

production systems protected by properly configured firewalls, intrusion detection and prevention products, etc.? Are operating systems, network devices and applications patched in a timely fashion to ensure protection against emerging attacks?

- Is an effective incident response team in place that can quickly detect, contain, stop and remediate an attack without significantly damaging business operations?
- Does the company's crisis management plan include processes for communicating with customers if and when an attack occurs? The plan should include who decides what gets communicated, by whom and when. Most cybersecurity professionals today will say that the question is not if a company will be breached, but when. The Verizon report noted that the vast majority of companies find out they have been breached when someone else tells them, usually a customer or partner. Companies should have processes in place to handle communications if a customer calls to say they think a breach has occurred – or worse, that the customer has been breached and they think it was through the company.
- Does the company retain any "sensitive" data – personally identifiable information (PII) or protected health information (PHI)? If so, it has regulatory obligations. This is in addition to HIPAA obligations if it has health care information about its employees.
- A company should do a cybersecurity review of its products as they would be implemented. Many cybersecurity consulting firms can do this. Based on that review, it should implement the measures that are necessary to protect

the firm and its customers. Once that is done, it should do a penetration test to see if anything was missed. The same vendor that did the review may be used, but it is often good to have a "fresh pair of eyes" look at the situation.

Donn Parker is the dean of information security/cybersecurity professionals, and he espoused a theory years ago that basically said that you cannot tell who might attack you, or what their method or motivation might be, so the best that can be done is to exercise "due care" (what a reasonable and prudent person or corporation might do) and be prepared to respond when necessary. Today, a company may know a lot about who might attack, and what the method and motivation might be, but it still needs to exercise due care and be ready to respond quickly and effectively. ■

Back to TOC

Dave Cullinane (davidmcullinane@gmail.com) is a co-founder of TruSTAR (www.trustar.co), a member of the Cloud Security Alliance Board of Directors (www.cloudsecurityalliance.org), and a member of the SIA Cybersecurity Advisory Board. ✉

The SIA Cybersecurity Advisory Board has compiled the top 10 causes of cybersecurity failure in systems.

Beginner's Guide to Product and System Hardening

From the SIA Cybersecurity Advisory Board

The SIA Cybersecurity Advisory Board recommends a few basic safeguards to help protect security products, systems and services against cyber attack. This is by no means an exhaustive list. Cybersecurity processes and technologies are constantly evolving along with the threats; the following can serve as the beginning for a larger cybersecurity plan.

These are the top 10 causes of cybersecurity failure in systems:

1. Inadequate security policy and process governance

- Establish a department or a team that responds to reported threats.
- Provide a way for end users and integrators to report found risks.
- Develop a framework as to how reported threats are discovered, fixed and taken out of production.

2. Reliance on "security through obscurity" – assuming that nobody will ever test security

- Assume that all of your security will be tested.
- Use proven ports and protocols.

3. Inadequate software and firmware patching; inadequate testing of patches before installation

- Authenticate patches; verify the update source is trusted.
- Use patch management tools.
- Include patches and software versioning in your change management practices.

4. Unencrypted, unauthenticated and uncontrolled wireless communications within systems

- Proceed like the network is untrusted.
- Remember wired is always more secure.

- Bear in mind denial-of-service protection is more critical when using wireless solutions.
- Default to HTTPS.

5. Unencrypted, unauthenticated and uncontrolled communications between systems

- Default to HTTPS.
- Filter IP addresses.

6. Poor password hygiene and insufficient segmentation of control system networks

- Disable default passwords.
- Require strong passwords before other configurations.
- Use password-tracking tools when available.
- Segment roles and responsibilities. (Do not use administrator privileges for non-admin duties.)

7. Lack of auditing and audit monitoring on networks

- Periodically audit the number of network connections.
- Periodically audit network connection lengths.
- Use information from these audits to target anomalies.

8. Control system networks shared with other traffic

- Ensure security networks are enterprise grade.
- Patch regularly just as other enterprise networks are maintained.
- Use of one network with mixed signals can be risky. When possible, segregate networks either physically or logically (VLAN).

9. Poor coding of control system software causes failures

- Enable application whitelisting.
- Filter out dangerous executables.

10. Lack of configuration management and tracking for hardware and software

- Remove dormant code from firmware.
- Track hardware and software versions when products leave the warehouse.

The Cybersecurity Advisory Board was launched by the Security Industry Association in 2015. More information is available by contacting SIA Standards Director Joe Gittens (jgittens@securityindustry.org). ✉

SIA Technology Insights Article List

All of the articles published by *SIA Technology Insights* since it was launched in 2013 are listed below by subject. The edition in which an article was published is noted after the title:

S16: Spring 2016	S14: Spring 2014
F15: Fall 2015	W13: Winter 2013-14
S15: Spring 2015	J13: June 2013
F14: Fall 2014	

All editions are available at www.securityindustry.org/techinsights.

Access Control/Identity Management

From Legacy Systems to Advanced Access Control (F15)
New solutions can offer extensive benefits to municipalities
By Robert Laughlin, Galaxy Control Systems

Unlocking the Door (F15)
Next-generation access control systems can offer new insights and greater security
By Scott Sieracki, Viscount Systems

Striking the Balance Between Security and Safety (F15)
Classroom door locks are invaluable, but they must allow quick egress
By Mark Berger, Securitech

Get Up and Bar the Door (F14)
Access management and door hardware play a critical role in school security
By April Dalton-Noblitt, Allegion

Who Is Entering Your Facility? (F14)
Verifying identities is challenging; partnerships can help
By Daniel Krantz, Real-Time Technology Group

Say Hello to Social Spaces (S14)
Social Applications will transform the security experience
By Steve Van Till, Brivo Systems

Fingerprint Biometrics for Secure Access Control (S14)
Moving beyond passwords and tokens can enhance security while decreasing costs
By Consuelo Bangs, MorphoTrak

Integrating Card Access with Interlocking Door Controls (S14)
While there may be implementation challenges, interlocks can greatly enhance portal security
By Bryan Sanderford, Dortronics Systems

Frictionless Access Control: A Look over the Horizon (S14)
New uses of biometric and RFID technologies could make access badges obsolete
By Henry Hoyne, Northland Controls

More Security, From Bottom to Top (S14)
Buildings are increasing entrance controls on the main floor and upstairs
By Tracie Thomas, Boon Edam

Hardware Security, Today and Tomorrow (W13)
Advances in door technology are enhancing both safety and convenience
By Will VandeWiel, DORMA Americas

Secure Authentication without the Cost and Complexity (W13)
New technologies are narrowing the gap between passwords and stronger authentication solutions
By Ken Kotowich, It's Me! Security

From Access Control to Building Control to Total Control (W13)
How innovation drives the need to update product standards – and ways of thinking
By Michael Kremer, Intertek

The Technology Behind TWIC (J13)
Smart cards are finally getting smart readers, but how will it all work, and how will it connect with existing PACS?
By Walter Hamilton, Identification Technology Partners

Big Data

Transforming Data into Actionable Intelligence (F15)
New solutions can identify insider threats before it is too late
By Ajay Jain, Quantum Secure

The Evolution of Risk (F15)
Banks are using analysis of 'big data' to enhance security
By Kevin Wine, Verint Systems

Reducing Retail Shrink with Business Intelligence Software (F15)
Data mining can be a valuable new tool for loss prevention professionals
By Charlie Erickson, 3xLOGIC

Cybersecurity

IoT Makes New Security Partnerships Essential (S16)
Bringing physical security and IT security together can enhance both
By Rob Martens, Allegion

Because You Can Never Be 100% Cybersecure (S16)
Effective use of strategies for countering attacks can minimize risk
By James Marcella, Axis Communications

Becoming Predictive, Rather than Reactive (S16)
A holistic view of physical and logical identities can help to identify insider threats
By Don Campbell, Quantum Secure

A Standard Response to IoT's Security Challenges (S16)
Technical standards are essential to securing billions of connected devices
By Steve Van Till, Brivo Inc.

Don't Be the Weakest Link (S16)
Security, IT departments must work together to reduce vulnerabilities
By Stuart Rawling, Pelco by Schneider Electric

Creating a Cybersecure Physical Security Enterprise (S16)
Simplicity and convenience are the enemies of security
By Paul Galburt, IPVideo Corporation

A CEO's Guide to Cybersecurity (S16)
Identifying and addressing vulnerabilities must be a priority
By Hans Holmer, Intelligent Decisions

Tackling the Complexities of the Connected World (S16)
Enterprise security must be a team effort
By Herb Kelsey, Guardtime

The Importance of Practicing 'Due Care' in Cybersecurity (S16)
Taking appropriate precautions can prevent security equipment from being a cyber vulnerability
By Dave Cullinane, TruSTAR

Beginner's Guide to Product and System Hardening (S16)
From the SIA Cybersecurity Advisory Board

Keeping the Security System Secure (F15)
Ensuring that video stays online is key to managing risk
By Bud Broomhead, Viakoo

Target, eBay … and You? (F14)
Cybersecurity threats are real, even for small businesses
By Hank Goldberg, Secure Global Solutions

Electronic Security Meets the Ecosystem (J13)
IP devices increase both rewards and risks. How secure is your system?
By Pedro Duarte, Samsung Techwin

Fire and Life Safety

Removing the Barriers: The Wireless Side of Fire Protection and Life Safety (S15)
The industry's wireless movement is fueling innovation
By Richard Conner, Fire-Lite Alarms and Silent Knight

The (Slow) Transition to IP in Fire and Life Safety Devices (J13)
Codes and regulations often force fire and life safety equipment to use older technology, but that is changing
By Christopher Peckham & Walter Frasch, Kratos Public Safety and Security Solutions

Integration

Commanding the Enterprise (S15)

New software platforms enable security leaders to ensure awareness, manage risk

By Rob Hile, SureView Systems

Tying It All Together (S15)

Integrating video surveillance, access control, building management and other systems can enhance security and reduce costs

By Mitchell Kane, Vanderbilt Industries

Safe on the Water (S15)

Integrated solutions secure the nation's largest independently owned commuter ferry operation

By Kostas Mellos, Interlogix

Broken Promises: The Current State of PSIM (F14)

Physical security information management solutions have so far fallen short of expectations, but next-generation systems could change that

By David Daxenbichler, Network Harbor

Enhancing Continuity Planning through Improved Security (F14)

Web-based systems can tie everything together

By Kim Rahfaldt, AMAG Technology

Technology-Enabled Collaboration Builds Safe Cities (S14)

Better management of more information can enhance the protection of people and property

By Itai Elata, Verint Systems

Solving a Big Problem for Small Businesses (W13)

New security technologies offer integrated solutions for small and medium enterprises

By Scott McNulty, Kantech

Intrusion Detection/Alarms

Integrating Intrusion (S15)
Video and access have converged on the network; the time has come for intrusion detection to join them
By Mark Jarman, Inovonics

Integrating Technology with Telephone Service at Central Stations (W13)
IVR implementation can be challenging, but when done well, it can significantly increase capacity and customer satisfaction
By Jens Kolind, Innovative Business Software

Related Issues

Maintaining Power (F15)
New network communication solutions can minimize system downtime
By Ronnie Pennington, Altronix

Do You Hear What I Hear? (S15)
Audio technology is redefining the surveillance industry and has become an essential component of security systems
By Richard Brent, Louroe Electronics

Enabling Safe Learning Environments (F14)
Securing schools demands a layered approach
By Neil Lakomiak, UL

From Horse-Drawn Wagon to Moving Truck (F14)
Nearly a century after the first VBIED was detonated in the U.S., what can be done to mitigate the risk of car bombs?
By Laurie Aaron, Building Intelligence

What Is in Store for the Physical Security Community (S14)
New technologies will open up great opportunities for the industry
By Bill Bozeman, PSA Security Network

Security and Privacy in a Connected World (J13)
With proper planning and precautions, security and privacy can complement – not compete with – each other
By Kathleen Carroll, HID Global

A Case for a Green Security Landscape (J13)
Sustainability can be good for both the environment and the bottom line
By John Hunepohl & Aaron Smith, ASSA ABLOY

Video Surveillance

Big Video Data (F15)
Video management systems offer a powerful platform for security and business intelligence
By Jeff Karnes, 3VR

The Public Safety Data Lake (F15)
Making the right decisions regarding storage and other issues can vastly increase the value of video surveillance
By Ken Mills, EMC

The Sun Shines on Surveillance (S15)
Solar power enables wireless video solutions in remote locations
By Dave Tynan, MicroPower Technologies

Surveillance in the 21st Century (S15)
Smart, 3-D, 360-degree cameras that see in the dark are on the way
By Jumbi Edulbehram, Oncam Grandeye

10.7 Billion Security Challenges (S15)
As transit ridership increases, so must security
By Steve Cruz, Panasonic

The Future of Video Surveillance (S15)
A rapidly changing security landscape will provide new ways to meet end users' needs
By Alex Asnovich, Hikvision USA

Making Campuses Safer with Innovative IP Technologies (S14)
Networked systems mean more information, more collaboration and more security
By Kim Loy, DVTEL

Harnessing the Increasing Power of Video (S14)
New functionalities and greater ease of use enhance the value of video in both security and non-security applications

Megapixel Cameras Go Mainstream (W13)
Functionality, versatility, clarity make megapixel video the future of surveillance
By Scott Schafer, Arecont Vision

Seeing the Big Picture: 360-Degree Camera Technology (W13)
High-resolution panoramic video overcomes the limits of PTZ cameras
By Steve Malia, North American Video

Achieving IP Video Management System Scalability through Aggregation (W13)
Video isn't just about security anymore
By Jonathan Lewit, Pelco by Schneider Electric

What's New on the Video Surveillance Front? (J13)
A keener eye, a longer memory and a sharper IQ
By Fredrik Nilsson, Axis Communications

Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security (J13)
As technology advances and prices fall, thermal cameras have become a cost-effective way to secure the perimeter
By John Romanowich, SightLogix

Video Analytics in the Modern Security Industry (J13)
Analytics can make cameras smarter, but how smart can they get?
By Brian Karas, VideoIQ

The Untapped Benefits of Recorded Video Surveillance (J13)
Recorded video holds a wealth of information that can be used not only post-event but also proactively. Fast video review makes accessing this data possible
By Rafi Pilosoph, BriefCam

SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, Md. All editions are available at no charge at www.securityindustry.org/techinsights. Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

securityindustry.org/techinsights

Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
301.804.4700