High-Powered
A roadmap for securing dams

Changing Credentials Forever
Could your smartphone replace the access fob?

Cover Your Bases
Protecting security equipment from cyber risks

SIA

Insights

TECHNOLOGY

Exclusive Women in Security Edition

Volume 6, Issue 2
Fall 2018

Welcome

Dear Reader,

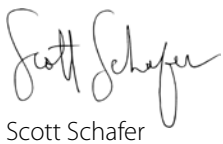
In each issue of *SIA Technology Insights*, we look to the leading edge of security technology, covering applications and solutions and highlighting the latest thinking from top experts on applying today's security technologies.

Although security technologies are continuing to evolve, there is still a need for greater diversity in the industry. The benefits of a diverse workforce are many: according to a McKinsey report examining 180 companies over the course of two years, diverse boards' returns on equity are 53 percent higher than those of companies in the bottom quartile of diversity, and a Massachusetts Institute of Technology (MIT)-George Washington University study of 60+ offices found that an office with an equal male-female split would be associated with a 41 percent revenue gain. As Facebook executive Sheryl Sandberg said in her commencement speech to MIT's graduating class, "There are still skeptics out there when it comes to the value of diversity. They dismiss it as something we do to feel better, not to be better. They are wrong. We cannot build technology for equality and democracy unless we have and we harness diversity in its creation."

SIA's Women in Security Forum, a new initiative offering programs, professional development opportunities and networking events, is designed to support the participation of women in the security industry. As part of this effort, this special edition of *STI* shares exclusively women-authored content. We hope to showcase the accomplishments and insights of female leaders in this space, help change persistent stereotypes and help pave the way for greater inclusivity within the industry. We hope these articles will inspire both women early in their security careers and those interested in entering the industry.

In this issue, you'll find exclusive content on the latest security trends and topics, including vehicular attacks, managed services, outdoor lighting for video surveillance, protecting power-generation dams and the cybersecurity of integrated physical security systems. You can find this edition and past issues of STI online at securityindustry.org/techinsights. We welcome your feedback on these articles and encourage you to propose your content for future issues and contact us at info@securityindustry.org.

Sincerely,

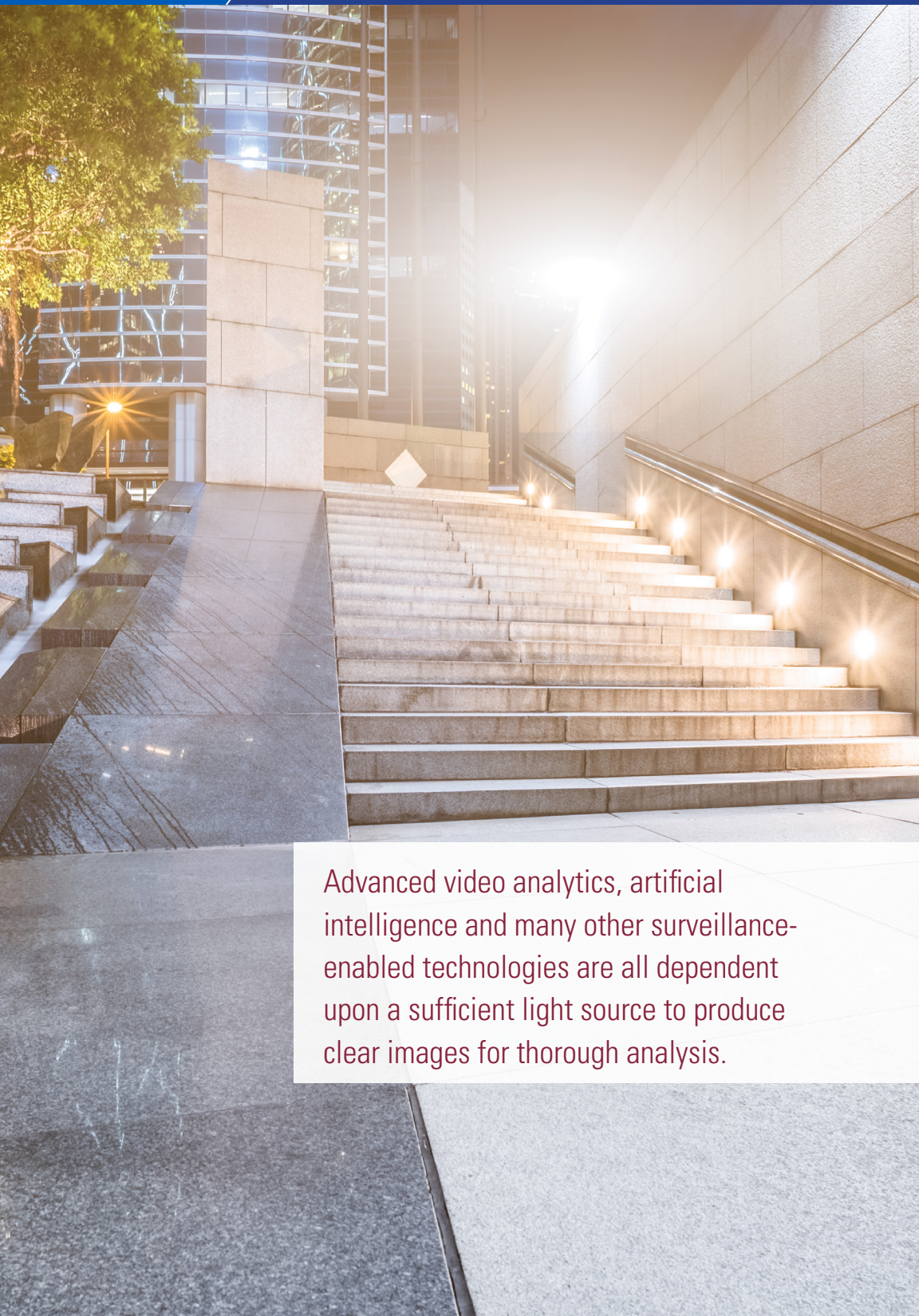


Scott Schafer
Chairman, Board of Directors, SIA

Don Erickson
CEO, SIA

Table of Contents

Search the SIA Membership Directory



Advanced video analytics, artificial intelligence and many other surveillance-enabled technologies are all dependent upon a sufficient light source to produce clear images for thorough analysis.

Lighting the Way to a Smarter, Safer City

The Importance of External Illumination Systems When Lighting for Video Surveillance

By Eddie Reynolds
Iluminar, Inc.

Demand for video surveillance systems has continued to surge throughout the years, with its market share expected to reach $40 billion by 2019 according to TrendForce's market data. While there is no doubt that cameras keep us safer and aid in law enforcement efforts, their effectiveness, specifically in low-light applications, is often called into question. With the rising popularity of advanced video analytics and artificial intelligence (AI)-enabled solutions, image quality and clarity has never been more important. Additionally, "smart" technologies are being added to bolster the security of major cities around the globe.

Often overlooked are lighting solutions that make it all possible, allowing for superior image quality no matter what time of day or night, and

enabling all smart city technologies that are currently high in demand.

With large metropolises continuing to grow, there is a need for better security to improve basic operations, traffic flow and overall public safety. Specifically, there is a need for

advanced video surveillance and video analytics, typically the "bread and butter" of security systems.

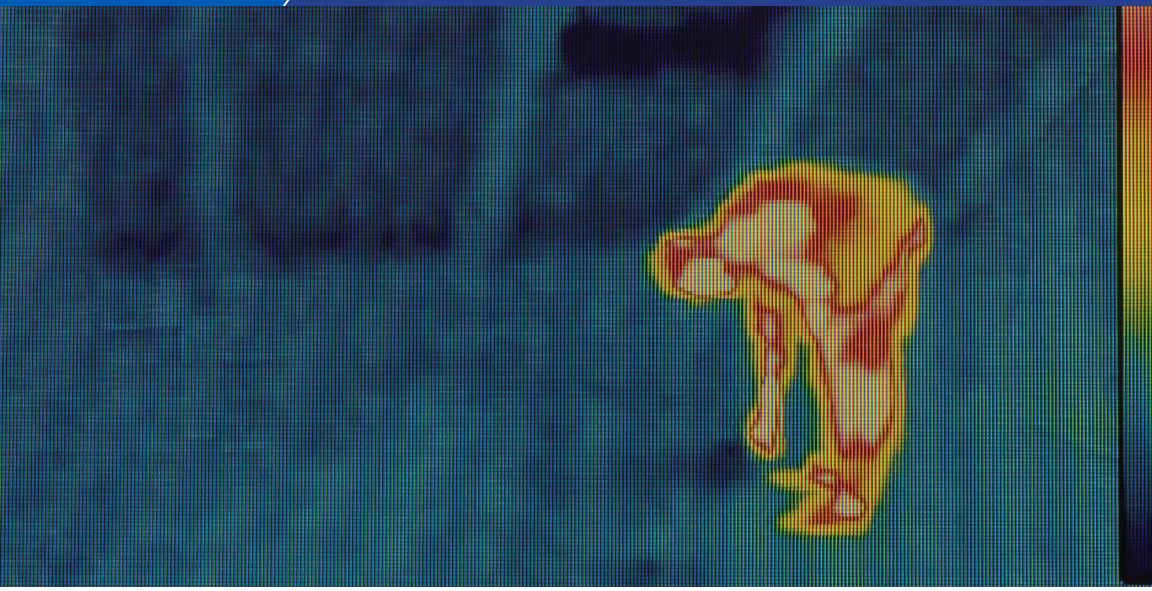
One of the most common pitfalls of these video solutions is inadequate lighting, resulting in unusable video in low-light conditions. Without sufficient lighting, video cameras are rendered ineffective, and the dark, grainy footage they capture is unusable by both security personnel and the analytic platforms enabling advanced functions. Inadequate lighting not only hampers video surveillance efforts, but also provides the perfect camouflage for criminals who are looking for easy opportunities.

Seeing Clearly

Illumination plays a pivotal role in the overall effectiveness of video surveillance systems; this is because cameras, much like the human eye, need some form of light to "see", or capture video. While it may seem obvious, it's important to acknowledge that darkness greatly diminishes a cameras ability to perform, and, as a result, there is far less situational awareness and a much greater chance for security blind spots to occur -- leaving assets vulnerable to attacks.

The common response is to place cameras near regular streetlights or emergency lights, but this approach can have its own drawbacks. Not only do these sources sometimes not provide enough light, but they also may not be strategically placed to optimize object capture and monitoring.

Advanced video analytics, AI and many other surveillance-enabled technologies are all dependent upon a sufficient light source to produce clear images for thorough analysis. Everything from simple motion detection to facial recognition and license plate reading



is ineffective in the absence of light. Not only that, but unclear images often result in false alarms, wasting valuable time and resources, ultimately preventing law enforcement from responding to true threats.

Harnessing the Power of White Light (LED) and Infrared (IR) Lighting

So what are the best lighting options for security applications? Most lights fall into two categories: LED and infrared lights, each coming with their own set of benefits depending upon the deployment. When exploring lighting options, knowing the needs of the application is key to finding the right fit.

White light illuminators harness visible light to brighten the area in full color, which both deters crime by eliminating the cover of darkness and enhances video for target identification. For more covert surveillance applications, IR illuminators have a much longer range and are completely invisible to the human eye. LED is most often used for illuminators, having 80-90 percent efficiency, as compared to the 10-20 percent for incandescent, halogen, and fluorescent. On average, the efficiency of commercial and public LED lighting saves the user over $700 per year per bulb, while simultaneously delivering superior illumination quality, providing an even spectrum of light without blind spots.

> External IR illuminators provide superior range for long-distance video applications, with some units allow for ranges of over 900 feet.

While convenient, cameras with built-in lighting options provide their own set of challenges to work around.

The most commonly used integrated IR illuminators in day/night cameras are only effective for short distance applications, providing light for up to 100 feet at most. Built-in LEDs around the camera lens can also pose serious issues, causing the camera itself to overheat and the bulbs to burn out and attracting bugs to the camera lens with the positioning of the light.

On the other hand, external IR illuminators provide superior range for long-distance video applications, with some units allow for ranges of over 900 feet. Because these light sources are installed separately from the camera, the security camera has greater bandwidth for video storage. Another advantage of independent white light and IR illuminators is they are available in a variety of angles, one important system design aspect that is often overlooked. Deploying a light whose angle of illumination directly corresponds with the camera lens eliminates hotspots, meaning end users can enjoy evenly lit, clear images.

When thinking of all of the "smart" technologies that go into making cities safer, like AI and deep learning software, it's important to note illumination's role in making it all possible.

Safer, Smarter Cities

When thinking of all of the "smart" technologies that go into making cities safer, like AI and deep learning software, it's important to note illumination's role in making it all possible. Whether it is securing businesses, campuses, or hospitals within a city, functioning analytics improve overall visitor management for any facility. External illumination enables advanced functions, including facial recognition, people counting and license plate recognition, to work together and perform at their best.

Take, for example, facial recognition, a technology that is positioned to have a major impact on the security industry. These analytics can be integrated with existing cameras but cannot function properly in low-light scenarios without additional lighting. Imagine someone trespasses onto a closed college campus after hours and approaches a library. In this scenario, a wide-angle short-range white light illuminator has been mounted alongside an HD camera to aid facial recognition software at the library's entrance. As the individual approaches the library, the camera scans the person's face, running it against a list of registered sex offenders. The camera identifies a match and sends an alert to the campus security director. Before the situation can escalate further, law enforcement is dispatched, the individual is detained, and a potential threat is prevented. The facial recognition analytics would not have been able to perform if it were not for the external illumination allowing

the cameras to "see" the suspect as they approached a secured area of the campus.

License plate recognition (LPR) is another advanced analytic software gaining traction in the public safety and security market. Capturing license plates has proven to be a major point of pain for all video surveillance solutions. Images captured are usually obscured by reflections from the sun or other headlights. Many IP cameras can now enable LPR by simply adding an external lighting fixture. This means that cameras can detect license plates in low-light or no-light scenarios.

Not only does this ensure that blacklisted individuals do not enter facilities (hospitals, airports, casinos, etc.) but it also aids in the recovery of stolen vehicles. In the U.S., a vehicle is stolen every 45 seconds, and nearly 42 percent of those vehicles are never recovered, as reported by the National Highway Traffic Safety Administration (NHTSA). By strategically placing LPR-enabled cameras around a city, law enforcement would be able to track the whereabouts of stolen vehicles by flagging them within the system. When the license plate of a stolen car has been scanned, authorities can immediately be informed of the vehicle's location within the city.

Deterring Crime and Aiding Law Enforcement

When it comes to the safety of other city infrastructure, many government buildings and campuses face vandalism crimes regularly. For some, the presence of graffiti creates a sense of unease and lack of protection, and an estimated $12 billion a year in public funds are allocated to the removal of graffiti in the United States

alone, according to data from the Department of Justice's Community Oriented Policing Services (COPS) program. This vandalism contributes to major losses in revenue triggered by decreases in property value, unsellable retail merchandise and even a decrease in passengers on public transit. All of these situations can cause interruptions in business operations and financial losses.

The Impact of Lighting Color on Security

Believe it or not, some lighting can encourage criminal activity depending on its color. Dim yellow lighting not only hinders video surveillance performance, but it also often makes people feel uneasy, as reported by Buildings.com in the 2017 article, "Who's Watching Your Facility." However, white light illumination with a color temperature rating of 6500k does the opposite, filling dark areas with inviting bright light and affording better situational awareness. When white light illuminators are strategically placed in dark, regularly-targeted areas, the white light can act as a deterrent and communicate the sense of "being watched." As a result, vandals can be dissuaded from committing crimes. White light has also proven to be highly effective in aiding in the illumination of crime scenes for judiciary purposes. This bright white lighting naturally enhances full-color video capture, aiding tremendously in suspect identification and apprehension. IR light, on the other hand, may not be a crime deterrent but works effectively to enhance and enable advanced functions for city surveillance at night.

Best Practices for Integration

Having the right illumination for security surveillance goes far beyond flooding a given area with light. Illuminators must be strategically placed to obtain optimal results, and where security operators can truly see the benefits in the surveillance footage. Here are some best practices for illuminator deployment.

The first step is taking the time to carefully assess the environment and selecting the right light for the deployment. So how can you tell what light you need for applications? Generally speaking, white light illuminators are most effective in applications where deterring crime and capturing evidentiary class video for suspect identification are the priorities. White light is best used in places like parking lots or garages, loading bays, airports or other areas where color video is crucial.

IR lighting is ideally used when the deployment calls for covert monitoring, not alerting intruders that they are being watched. Common IR applications include securing borders, government facilities and critical infrastructure sites. An IR security light allows authorities to track intruders' movements without them knowing, revealing their point of entry.

> When white light illuminators are strategically placed in dark, regularly-targeted areas, the white light can act as a deterrent and communicate the sense of "being watched."

Lastly, knowing what type of camera is being paired with illuminators is another key factor in deployments. Pan-tilt-zoom (PTZ) cameras, which are becoming less popular but are still used in some installations, present their own set of unique challenges, as their ability to move cannot be matched by lighting solutions. This is where angles of illumination come into play. For a PTZ camera, the key is to match the angle of illumination with their required scene of view to obtain full coverage. For example, by setting multiple 120-degree wide-angle external illuminators on a triple-mounting bracket, complete coverage for a 360-degree camera can be achieved.

Many people are still in the dark when it comes to pairing external lighting and surveillance solutions. Without ample light, video capture is impossible and all advanced analytics functions rendered useless. With the growth of both "smart" technologies and cities, the video market will only expand, opening new doors for security analytics. ■ **Back to TOC**

Eddie Reynolds (eddier@iluminarinc.com) is CEO and president of Illuminar, Inc. (iluminarinc.com)

Search the SIA Membership Directory

With the introduction of biometric and smartphone credentials, the lifespan of legacy physical access control credentials is quickly reaching an end.

Overcoming Objections to Smartphones as Your Credential

Could the phone replace your access control card or fob?

By Suzi Abell
3xLOGIC

Moore's Law notwithstanding, technology advances have always outpaced our ability to adopt and consume them. This has been and remains the case with even the least complicated aspects of technology like electronic access control (EAC). At their most basic level, EAC systems lock and unlock the door, a simple task until you mix in people who need schedules and rules and exceptions to the rules and on it goes. It is often difficult to drive the desired behavior and this is particularly true with the credentialing that is an integral part of an EAC system. Initially, a credential might have consisted of a simple numeric code that was entered into the lock, often referred to as a cipher lock, thus allowing access. This was a terribly insecure and difficult-to-manage solution, and has since

evolved into physical credentials, which expanded to include fobs, proximity cards, biometrics and now a smartphone app playing the role of credential.

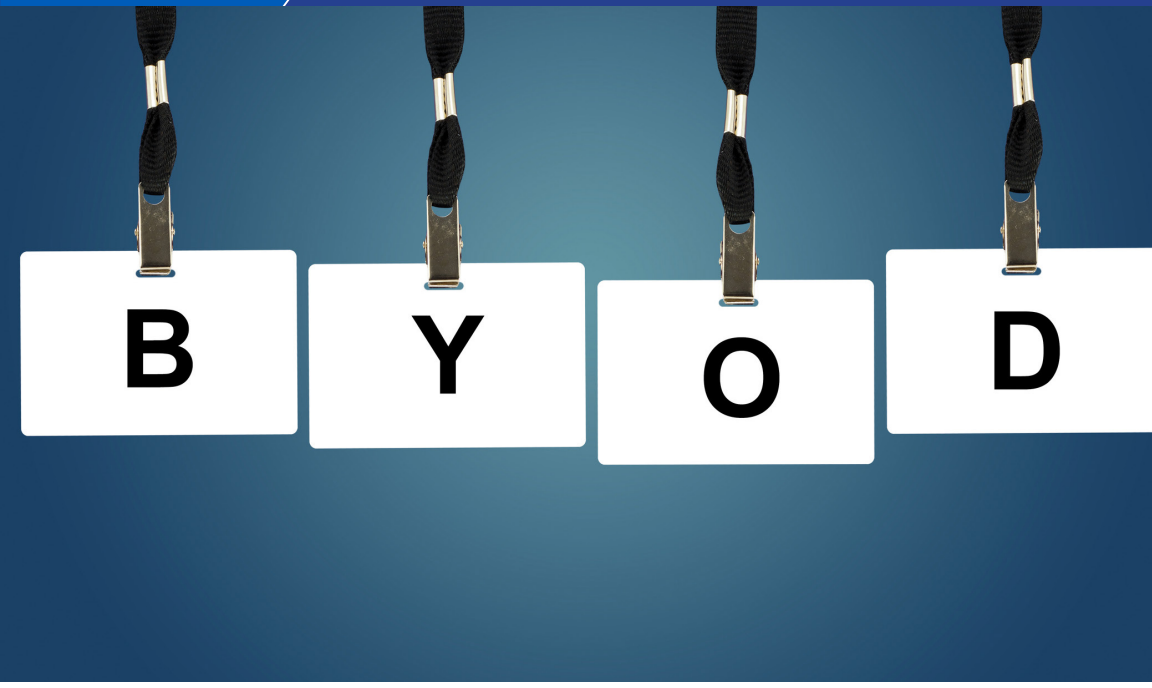
With the introduction of biometric and smartphone credentials, the lifespan of legacy physical access

control credentials is quickly reaching an end. A convergence in physical and logical access control is driving completely new and different behaviors, as evidenced by the entry of players such as August, which was recently purchased by the largest lock and credential company in the world, Assa Abloy. This aquisition demonstrates validation for these changes in the way we provide access to our facilities.

In the very near future, everyone will carry a credential of some sort, and a mobile credential, housed on a smartphone, is a highly viable way to address these needs.

Smartphone as Credential: The Only Way to Go?

In an ever-accelerating trend, estimates show that 90 percent of the wireless locks sold are integrated with other smart devices. It's no longer necessary to struggle to manage a variety of insecure and vulnerable physical credentials when you can manage all of that through a mobile app. As this market expands into non-traditional access control applications, the necessity for an access control credential on an ubiquitous mobile device becomes mandatory. In the very near future, everyone will carry a credential of some sort, and a mobile credential, housed on a smartphone, is a highly viable way to address these needs.



There are four main drivers for a smartphone as your credential:

- Smartphone-based credentials are inherently more secure
- Smartphone credentials can do so much more
- Smartphone-based implementations can significantly reduce installation costs
- Smartphone-based credentials are nearly impossible to clone

Objections Real and Overblown

For any new technology, there will be naysayers. Some of those dragging their feet object because the new technology threatens their business models. Others just don't like change or tend to evolve ever so slowly. However, other objections do have validity and need to considered. How can you tell the difference?

Since the potential for smartphones as your credential burst on the scene a few years ago, much has changed. What were once valid objections or limitations have now been surmounted. Some examples:

- **Cards Are Cheap:** Mobile phones, even inexpensive ones, are roughly 20-40 times the cost of a card. And the cost of maintaining a phone is much higher, requiring frequent recharges and software updates while a card remains very inexpensive and essentially free to maintain once issued. **Reality:** Mobile credentials have the potential to make credentials more affordable by leveraging an asset that the vast majority of people already have (see http://www.pewinternet.org/fact-sheet/mobile/). In

addition there is the potential for reducing shipping and labor costs from managing cards that are frequently lost and/or misplaced.

- **Bring Your Own Device (BYOD) Is Awkward:** BYOD, or the fact that users leverage their personal phones for commercial uses, presents numerous problems, from network security to whether or not phone owners are willing to permit employer provisioning and/or management oversight. **Reality:** BYOD is a fact of life, and while personal devices will bring some complications, how often do you hear of a company issuing an employee a phone? And if a company does provide a phone, it's now a smartphone that can deliver a mobile credential in a corporate-controlled environment. The security industry is not the only one seeing this change. Retail is moving toward near field communication terminals to allow customers to use their smartphones in place of their debit/credit cards through Apple Pay, Samsung Pay and Android Pay Apps.
- **Ongoing Service Billing:** What happens if the phone bill is unpaid and the employee incurs service interruption? **Reality:** Smartphones have become so ubiquitous and, for nearly every employee, so essential to day-to-day, hour-to-hour operation that one's phone bill is probably the very last bill a person will leave unpaid.
- **Technology Limitations:** The wide range of technical issues

that can go wrong with a mobile phone cannot be easily dismissed. Even problems as basic as battery power, operating condition, reliable function and even multi-tasking demands need to be considered. **Reality:** Everybody has a smartphone, and we all use these devices for so many essential functions today that there is ample incentive to make certain one's phone is operating in top condition.

Having dispensed with the above objections because they have been taken care of by time or technology advances or both, there are objections to smartphone as credential that do require further examination and discussion.

Valid Objections Have Their Day

The objections covered above are no longer valid in slowing down smartphone as credential adoption. Are there other objections that we must deal with? Yes, and they are as follows:

- **Physical Revocation Uncertainty:** Unlike plastic credentials that can be turned in and physically repossessed when employees are dismissed or turn over, mobile credentials must be remotely invalidated on a device that may remain unseen. **Reality:** A good mobile credential solution should not depend on sending an update to the phone to disable a credential, that should happen in real time whether the phone is connected or not. An efficiently-designed mobile credential integration will not depend on access to the physical mobile device to activate or deactivate the credential. In reality, access is granted by the interaction between the mobile credential and the extended access control (EAC) system. If the credential is deactivated in the EAC system, then access grants are denied without regard to the type of credential presented.
- **Awkward or No Picture IDs:** Unlike physical cards that are often printed with the user's picture, name and other basic identity details, these are very often hidden or obscured by phones. **Reality:** Yes, calling up a photo ID on one's phone does take more time than flashing a badge. But consider that many companies no longer even print identifying information on a badge for fear that the wrong person will get control of that badge and gain unauthorized entry. There are two main uses for badge pictures and two main philosophies around putting pictures and identifying information on credentials.
  1. Worn and visible at all times so a person can be readily identified as belonging.This is an area a mobile credential does not address.
  2. To verify that the person passing a secured portal is

indeed the person to whom the credential was issued. In this case, it's better to compare the photo stored in the system to the person, instead of a relatively-easy-to-forge picture on a badge. Also, a good mobile credential solution can implement multi-factor authentication (MFA), delivering much greater assurance that the person is who they should be.

Perhaps the most secure solution is to use a mobile credential for access and have PVC cards printed with the person's badge picture etc. that are just for visual verification and are not credentials.

Possible Other Objections:

- **Takes too long to get through a door.** The objection is that the user must pull out the phone and then launch an app. **Reality:** For mobile credentials that do not require close proximity to a reader, they will drive a change in behavior as users realize they can initiate the request as they approach the door, with the door unlocked by the time they reach for it. This negates the extra time required. Watch-based extensions to mobile credential apps also promise to speed up the process.
- **Phone could unlock remote doors.** Some people don't like being able to unlock doors 20 miles away, or even the potential to remotely unlock doors. **Reality:** A good mobile app should support geofencing to require users to be close to the door they are attempting to access.
- **Traditional credentials formats are always on, but phones can**

be turned off. The objection is simple: Users' phones can often be turned off and are therefore not appropriate as a credential. **Reality:** The average person has a high level of incentive to always keep their phone on and to know where it is. Why? Think of all the apps nearly every user is accessing on a minute-by-minute basis: A user's phone has their credit card, Facebook, Twitter, instant messaging, email and texting, navigation, to-do lists, camera, music and calendar, and the list goes on and on and on.

Benefits of a Mobile Credential Solution

- Mobile credentials are inherently more secure.
  - Credential holders are unlikely to share their mobile devices with others.
  - Mobile users are very aware of where the devices are at all times.
  - It is very difficult to clone a mobile device/mobile credential.
- Mobile credential apps expand the capabilities of the EAC system.
  - Group notification/ mass notification can be implemented directly to the credential holders' mobile devices.
  - Tracking of the mobile device can provide real-time location information for added security.
  - Mobile credential app can quickly become a bi-directional communication channel for personal security (PERS).

What's Your Single Largest Security Risk?

Forget about high-security credentials such as MIFARE and sophisticated certificate handshakes. The single largest security risk for access control is a valid credential in the wrong hands. When that happens, it doesn't matter if it's a 125KHz "dumb" prox card or the most sophisticated smart card; a potentially malicious user now has access, and no one will know if that lost card isn't reported.

The smartphone as the credential is significantly more secure because of one simple fact: People may not know the location of their access control credential at any given time, but they are intimately aware of the location of their smartphone at all times and this location can be tracked. Users are naturally much more careful as to whom they allow to hold or use their phone.

The World of Mobile Credentials

So, how is the world of credentials changing forever? A smartphone-based credential can be and do so much more. In the near future, we'll start to see features such as:

MFA

Smartphones already implement MFA. Soon, new mobile credential implementations will allow administrators to require a screen unlock pin/biometric/gesture to set up

a mobile credential, thus implementing MFA with no new hardware at the door.

Mass Notification

A credential – supporting two-way communication with active notification capabilities – can be leveraged to send automated or ad-hoc notifications to users. Add location services and geofencing capability, and you can send notifications only to those people who are within a specific geographic area. And you can further target those notifications to specific people.

Location Awareness

Stop treating a smartphone like a legacy credential; no one should ever "badge" a phone at a reader. By using location services, administrators will define how near to the door a person must be to request access.

Virtual Buttons

With an app for users that uniquely identifies them, why not give them more? We'll see the ability to add virtual buttons to an app to perform functionality specified by the administrator – and such buttons/functions will only be distributed to those allowed to use them.

Personal Safety/PERS

A mobile app that functions as the user's credential and provides two-way communications with a central monitoring station will also provide a path for two-way emergency communications. For example, an employee leaving the building at the

end of the shift on the way to her car can quickly and easily ask for assistance or notify security of a potential issue remotely via the mobile device in her hand.

Revoking a Credential

An administrator can disable a user's mobile credential at any time from the server with no need to access the actual smartphone. The smartphone app knows how to submit a credential request but has no idea how to unlock a door. Additionally, administrators can also remotely wipe smartphones of the mobile credential and related apps connected to a corporate network.

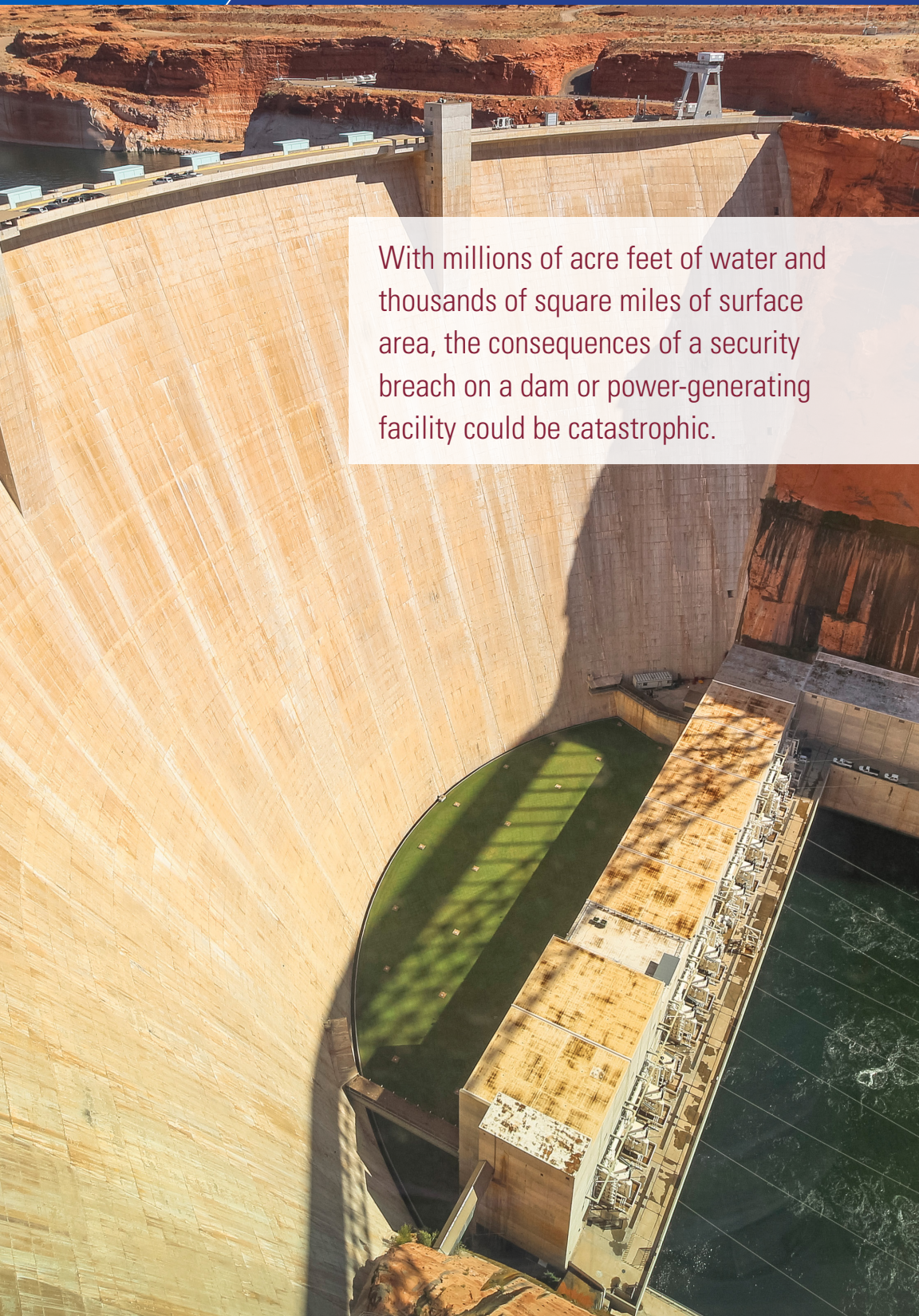
Lower Costs and Added Features

Finally, let's consider cost. A smartphone credential adds significant functionality over a traditional credential and is always upgradeable to add new capabilities – all for the same cost, or less, as that of traditional credentials. Also, users do not require a reader to enter a door, so enterprises can eliminate readers on most doors to keep the entrance looking clean and to reduce installation costs.

Over the next 24 months, we will witness unprecedented changes in the tools and services you use every day, and one of those tools will be your access control credential. The security of a door is only as strong as the management of the credential. It only makes sense for that critical credential to be secured inside the most highly encrypted device – your own smartphone. ■ **Back to TOC**

Suzi Abell (suzi.abell@3xlogic.com) is marketing manager for 3xLOGIC (3xlogic.com).

Search the SIA Membership Directory



With millions of acre feet of water and thousands of square miles of surface area, the consequences of a security breach on a dam or power-generating facility could be catastrophic.

The Process of Securing Dams

A detailed roadmap for securing dams and associated power generation stations

Yvonne Pire
Trofholz Technologies, Inc.

There are more than 90,000 dams and power-generating facilities in the United States, according to the U.S. Department of Homeland Security. These dams play a critical role in the infrastructure of our country, providing water for irrigation and for communities to drink, generating power that allows our modern lives to function, maintaining navigable waterways for transportation and freight and protecting our farms and communities from flooding.

With millions of acre feet of water and thousands of square miles of surface area and coastline, these assets are big, and the consequences of a security breach on a dam or power-generating facility could be catastrophic and far reaching. While there are obvious threats – including damage to surrounding areas and loss of services – the less obvious threats are just as critical. These facilities often create recreational areas that generate economic dollars for surrounding communities, thus the loss of function and changes to the landscape could endanger the livelihoods of hundreds

or thousands. Ensuring the security of these critical infrastructures is paramount for the protection of communities across the U.S.

Based on a decade of experience securing 33 dams and other power facilities in critical regions across the country, and having worked with agencies in California, Oregon, Washington and Georgia to support individual installations and networked water control systems, we at Trofholz have developed a standardized process to achieve the necessary security. At each site, it is necessary to balance the threats to the facility, the needs of the community and needs of onsite personnel. While each installation is different, security professionals can ensure they achieve a site's hardening goals by following a standard process while adapting the tools to meet the individual needs of each site. This process, with pre-project preparation, a site survey, a customized design plan, installation, testing and then cybersecurity and information assurance hardening, gives dams the full, integrated physical and information security system that is needed for this critical infrastructure.

Pre-Project Preparation: Everyone should begin each project by reviewing and understanding the appropriate national codes, standards, installation requirements and other applicable documents. On such critical installations, it is important to integrate compliance to regulatory requirements in to your project management plan. On government-run dams, it is often a requirement to have employees complete the Anti-Terrorism Level I awareness training. As a best practice, an operational security standard operating procedure plan should be established and tailored to each installation.

Site Survey: By conducting a site survey, the team can evaluate installed infrastructure, validate equipment quantities and identify any performance issues or operational limitations of the proposed system. With this information, the team can create a current site conditions report, which describes the site and facility, infrastructure, existing systems, equipment quantities and performance issues or operational limitations. This report can also address all regulatory compliance concerns, provide technical recommendations on improvements and list assumptions, giving the team a foundation to discuss the true needs of the facility, the specific dangers it faces because of its location, environment and role in the water system. These discussions will lead to the creation of a customized design plan.

Customized Design Plan: Prior to breaking ground with construction activities, the project will need thorough and accurate design plans that depict all electrical, civil, mechanical, electronic, excavation and infrastructure facets. This design plan should address the particular concerns of each location. Work on any installation could include the technology, electrical, civil and communications to support access control, intrusion detection and video management. More public sites may

On government-run dams, it is often a requirement to have employees complete the Anti-Terrorism Level I awareness training.

need vehicular crash barriers carrying U.S. Department of State K-12 crash ratings. All systems integrate into one common security management system (SMS) for ease of system monitoring and management.

Integrated Physical and IT Security: Many dam and power customers use truly integrated solutions with all access control systems and video surveillance delivered through single graphic user interfaces. To ensure successful performance, it is recommended to test multiple technologies in each terrain to ensure implementation of the most appropriate equipment and take advantage of the most advanced security tools available, combined into a user-friendly system. The system design should provide high system usability by integrating all technologies into a common SMS. Using a SMS ensures a system provides seamless, easy-to-use protection and management.

The SMS monitors and records to a database all system events, including authorized transactions, violation of either physical or virtual boundaries, procedural policies and system/equipment failures or malfunctions. The SMS allows separate groups to share a single database while partitioning the data through access permissions to maintain individual group security.

Based on the needs of the facility, a combination of pan-tilt-zoom (PTZ) and fixed cameras are typically used, chosen at the site survey in conjunction with the site security manager. Thermal imaging PTZ cameras and analytics may also be employed to support the desired security posture. At many facilities, the intrusion alarms are linked to cameras, so if a forced entry is detected, the nearest camera zooms in. A variety of intrusion-detection sensors are used, both indoors and out. Higher-risk facilities often install long-range acoustic devices, so security personnel can observe and deter intruders with pre-recorded messages or tones. The project will also include

physical security barriers, sometimes including fencing, crash bars, gates and bollards. The goal of consultants and integrations should be to support security assessments done by the site security manager, with the overall goal of increasing the posture and providing added security.

For some installations, a security control center (SCC) is used as the primary security monitoring and administration center. The SCC can be set up so the system can be expanded (scaled) to accommodate the monitoring and administration of additional remote security systems. In some cases, the primary SCC is combined with an additional secondary remote-client workstation as a backup.

Standard phone lines, microwave communications and wireless point-to-point solutions have all been used to ensure the systems remain interconnected.

Ensuring Communication: Most dam and power-generation facilities are not standalone sites but are part of a linked network. These sites are often remote and can have limited connectivity; while a few have some cell coverage, many are not even connected to landline, fiber or other communication networks. The team must adapt to coordinating with the available communication tools. Standard phone lines, microwave communications and wireless point-to-point solutions have all been used to ensure the systems remain interconnected. Dams are generally moving to centralized operations with only one main site in a string of sites staffed at any time. This means that the supervisory control and data acquisition (SCADA) and Generic Data Acquisition and Control System (GDAC) are dam controls, with all work done through programmable logic controllers (PLCs) and touch screens. With power generation and water levels controlled by a centralized location, the access control systems should follow suit; however, it is important to maintain the ability to monitor and administer each individual system locally.

Microwave communication is put in place with a router "network." The security system is included in the network. On multi-site or multi-facility dams, the facility separates the SCADA, GDAC and Electronic Security Systems (ESS) systems through the microwave. At each point/facility, there is a microwave, router and switch on site. A port on the facility router can be used for an additional router and second switch for the security systems. The security devices connect to the second route and bank of switches, creating a dedicated security network inside of the facility network. Microwave is useful when fiber is not an option because of the remote terrain or other limitations, and it is faster than phone lines when regularly maintained.

In other instances, wireless communication provides point-to-point radio communications, allowing the integrator to extend the network to

remote locations within each facility. Facility size and location play a huge role in communications challenges. Distance limitations on both fiber and copper create communication challenges and require different components to make each network connection work. Finding a solution to support system communications with the most effective and least disruptive results for the facility ensures the operator can achieve the highest level of facility hardening with the most on-site buy in.

Federal Identity Credential and Access Management (FICAM)/Federal Information Processing Standards (FIPS) 201 Compliant Systems: FICAM is the U.S. federal government's implementation of identity, credential, and access management (ICAM). It is meant to provide a common set of ICAM standards, best practices and implementation guidance for federal agencies. A FICAM/FIPS 201-compliant system begins with the readers. In a compliant system, the person requesting access goes through a two-factor authentication process. When the user presents the badge to reader, the certificate on the badge hits the certificate manager and sends a request to the federal bridge. The system receives a response from the federal bridge that the credential is either valid or invalid. A valid credential proceeds to the next step; an invalid credential is denied. If a valid credential is presented, the access request is then sent to the access control system. If the user is allowed in that area, the system unlocks the door; if not, the door remains locked and access is denied. In this system, all users must pass a thorough background check before the cards with certificates are issued.

Installation: Installation of security systems will typically require the use of above- and below-ground conduit throughout the entire facility, there is also the matter of high-voltage electrical distribution, fencing and gates. Each site follows a specific,

logical installation plan, keeping any existing security equipment in place and operational until the new system is online and functional. Civil engineering analysis can be needed to ensure proper foundation depths for towers and equipment, while still accounting for wind-load thresholds.

System Testing: When installation appears complete, contractor field testing (CFT) begins. During the CFT, all equipment is tested and calibrated, and the integrated systems are placed into service. After the CFT procedure, a detailed report is delivered to the customer describing the results of the system tests, diagnostics and calibrations and provides written certification that the system is calibrated and ready to begin performance verification testing (PVT). It is then recommended that the integrator conducts PVT and endurance testing and documents the results. During endurance testing, the goal is to identify all system failures, explain the cause of the failures and list the corrective action taken to repair the failure.

Quality: It is recommended that the quality control program works with and complements the U.S. Army Corps of Engineers' three-phase control system. Testing procedures will be performed and reports will document performance verification tests following quality assurance surveillance plans (QASPs). We include QASP tasks from the performance work statement (PWS) in our schedule and measure completion of these tasks against the performance objectives given in the QASP.

It is recommended that the quality control program works with and complements the U.S. Army Corps of Engineers' three-phase control system.

Cybersecurity and Information Assurance: The team should plan implementation, validation and accreditation of information assurance controls, including timely and effective configuration and vulnerability management. The team should develop and maintain the system security plan and artifacts for information security through receipt of accreditation. This ensures that administrators use information security engineering to implement or modify the information assurance component of the system architecture in compliance with the systems security plan and enforce accreditation decisions for information security. Because this data is so critical, the solution provider should work with the customer to develop a disaster recovery plan for this system and integrate the risk management framework into all systems, including hardware, software and other equipment. ■ **Back to TOC**

Yvonne Pire (yvonne.pire@trofholz.com) is CEO of Trofholz Technologies, Inc. (trofholz.com). Alison Smith (alison.smith@trofholz.com) of Trofholz also contributed to this article.

Search the SIA Membership Directory

The issue of protecting crowds of people from vehicles must now be considered a key issue for architects, planners and designers of urban public spaces.

Creating Invisible Security to Prevent Vehicular Attacks

Out of sight, out of mind – a new approach to mitigating vehicle terror attacks

Lara Valdur Eha
Marshalls Landscape Protection

The terror threat posed to the public has evolved dramatically over the last couple of years. Large-scale, meticulously planned bomb attacks have given way to vehicle assaults that target pedestrians. Concrete blocks and barricades – largely temporary measures – have been installed across the United States and Europe to protect areas of high footfall, national infrastructure and government buildings. But authorities in the U.S. and Europe must assign a greater role to design aesthetics when it comes to specifying the security measures that can prevent vehicle attacks.

In light of the clear shift in terrorist strategy, the issue of protecting crowds of people from vehicles must now be considered a key issue for architects, planners and designers of urban public spaces. We have seen a steep rise in the number of risk assessments carried out in towns and cities across the U.S. and Europe over the last 18 months, covering all types of infrastructure, buildings and events.

This new threat is significantly more difficult to predict. Rather than

face the risk of exposure of planning attacks over an extended period, terror organizations are now recruiting, encouraging and facilitating plots through remote supporters. Stripped down to the bare bones of an individual with motivation, intent and access to a vehicle, this type of attack has pared down the timeline between planning and execution to a matter of hours.

In reaction, we've seen authorities take a largely primitive and unsophisticated response. Large metal barricades, barriers and concrete blocks have become the default solution, providing an effective but very visible, fear-inducing method of protection. New installations of these barricades at Disney World in Florida, nuclear power stations and government buildings in Washington, D.C., together with those erected across London, Barcelona, Nice, Berlin and Melbourne, are cases in point. In October 2017, a man drove a rented pickup truck down a busy Manhattan sidewalk, killing eight people and injuring 11 others. Since the attack, New York City has spent nearly $65 million on protective measures, including the installation of 1,500 metal barriers in key locations around the central districts.

But while it's clear cities are taking the threat seriously, this type of protection makes the potential threat very visible to members of the public. This can create doubt, anxiety and create an environment of fear. Complaints from the public about this type of security measure have resulted in negative national headlines – for example, several stories in the U.S. and UK national press stated that new barriers erected at Disney World had turned the tourist destination into "a fortress."

Establishing an Environment of Fear

Creating this deep feeling of insecurity is a clear objective for the terrorists conducting the vehicle

attacks and, as such, those responsible for designing and securing urban spaces should not just be working to prevent them, but fighting against the psychology of terror, too. Stopping the threat is the priority, but addressing the impact of security measures among the public should be given strong consideration by those designing and securing cities from terrorist or criminal activity.

The human psychology behind this issue constitutes a vicious circle, with the higher perception of risk resulting in a greater threat felt by an individual. This theory applies directly to the presence of visible anti-terror security measures, such as the barriers and barricades we've seen erected over the last 18 months, which increase levels of suspicion, tension and fear among the public.

> Urban planners and designers need to consider how protective measures can be integrated into a town and city center without changing the way people feel about how they use a particular space.

This is a reaction that is hard-wired into the human brain. Anxiety worsens cognitive functioning, as our attention is drawn away from everyday life and towards something that is threatening and unusual. In effect, the very action of fortification is increasing the fear that people feel. It is clear that this type of hostile vehicle mitigation (HVM) measure could deter people from using highly populated

areas, such as shopping malls, theme parks and sports events, and that change would have a significant negative effect on businesses.

Giving Greater Focus to Design Aesthetics

The threat of terrorists targeting crowded public places provides authorities with a new and complex challenge. The need to create safe spaces offers those responsible for their design and protection a difficult compromise between maintaining the open, livable nature of the public realm and the necessity for security – especially in those cities and places that have built global reputations on the back of their visual appeal. This dichotomy – and our attempt to address the issue so far – does raise a fundamental question about how the inclusion of effective security changes the nature of the urban spaces we share.

Most security measures that we see being installed across the U.S. and Europe make little consideration for the design and aesthetics of an environment and represent a short-term approach when it comes to HVM. Their presence can radically change the nature of these spaces.

In her study *Invisible Security: The Impact of Counter-terrorism on the Built Environment*, Rachel Briggs writes: "It has been argued that 'security' has become the justification for measures that threaten the core of urban social and political life – from the physical barricading of space to the social barricading of democratic society – that rising levels of security in cities will reduce the public use of public space."

To prevent this, urban planners and designers need to consider how protective measures can be integrated into a town and city center without changing the way people feel about how they use a particular space. As

terrorists have rethought their tactics, designers of security measures like ourselves, have had to rethink the way in which we can mitigate vehicle attacks. The key question is how security can be more subtly integrated into the design of our public areas so it is unobtrusive, unthreatening and effectively hiding in plain sight.

Integrating Security Into an Environment

We believe that you can protect people and places from terrorism through landscape design and can do so in a way which is both effective and does not destroy the vibrancy of open, accessible urban spaces. Security should not just be about product specification. On a human scale, it requires a far more considered approach where the environment is created to intrinsically provide the protection people need, without an obvious show of "defense strength."

Thankfully, we're starting to see a shift in how urban planners and designers are tackling this challenge. Europe, and particularly the UK, is taking the lead. The UK's Centre for Protection of National Infrastructure has ensured that a requirement for aesthetic design is included as one of its six key guiding principles for delivering successful protective methods against vehicle attacks.

This forms part of a more multi-layered approach, which is not limited to simply introducing new objects or barriers to block attacks. Depending on the level of risk – which is often determined by the type of vehicle that can access the area and the speed it could reach – security should be considered at the outset and as a long-term solution. Firstly, designers and planners should evaluate the existing road infrastructure to keep

vehicle speed to a minimum, which can include various traffic calming measures, such as chicanes, bumps and restricted-width lanes, together with protected pedestrianized areas or water features that can slow approaching traffic in or close to highly populated spaces, or even prevent access entirely.

As a second step, security advisors should consider reinforced landscape furniture such as planters, seating, litter bins, lighting columns, cycle stands and bollards, which act as a far subtler final line of protection than fences, steel barricades and concrete blocks. Although these products look like regular landscape furniture, they are built with fortified PAS68 certified cores – the latest specification for barriers and bollards to assist in terrorism prevention, which specify a classification for vehicle security barriers and their foundations when subjected to impact. The foundations are built to varying depths, suitable for spaces with limited excavation and depending on the specified risk. Using the strongest specification, a single piece of furniture can stop a 7.5-tonne articulated lorry (equivalent to an 8.4-ton semi-truck and trailer in the U.S.) travelling at 50 mph.

> It is vital that future measures can be integrated seamlessly into a landscape while providing the necessary protection against vehicle attacks.

Delivering the Aesthetic Application

Taking an example of how this approach is now being implemented in the UK, Northamptonshire Police has secured the exterior of its new headquarters with landscape furniture that fits seamlessly into the surrounding landscape. Rather than fortifying pedestrian zones, the organization has used a range of bollards, seating, cycle shelters and bespoke tree planters to secure the area.

It's unsurprising that the increased threat from this type of attack has led to authorities scrambling to protect highly populated areas, landmarks and key infrastructure. For example, after the fatal shooting in Las Vegas in October 2017, the city installed hundreds of bollards along the Las Vegas strip in what officials called a "matter of life and death" to protect people from those who could use vehicles as weapons.

But while security has become a much higher priority when specifying a highly populated space, this is a permanent threat and the solutions used for HVM should be considered as a long-term response. Given the environment of fear, which steel barricades and concrete barriers induce and the knock-on impact this could have on business, it is vital that future measures can be integrated seamlessly into a landscape while providing the necessary protection against vehicle attacks. The focus should be on keeping this type of security out of sight and out of mind. ■ **Back to TOC**

Lara Valdur Eha (lara.valdureha@marshalls.co.uk) is product manager for Marshalls Landscape Protection (marshalls.co.uk).

When a breach occurs, each organization must take steps to learn from the outcome of other incidents and work toward strengthening the protocols in place for protecting breaches in the future.

Implementing Cybersecurity Best Practices in Five Steps

Concerned about the cyber risks of security equipment? Cover your bases with these practical recommendations.

Kim Loy
Vanderbilt Industries

The rapid gains that technology has made into everyday living have also changed how the security industry operates. In short, physical security has moved from being very simple inputs and outputs to encompassing always-connected devices, which makes the security industry very much a part of the Internet of Things (IoT) world. Of course, this leads to the question: How does physical security protect itself from cyber vulnerabilities?

There are already millions of smart home devices in the world, including smart alarms, locks, lighting, baby monitors, thermostats and televisions. It is predicted that there will be more than 21 billion connected devices by 2020. The amount of data that these types of IoT devices can create is huge: A Federal Trade Commission report,

Internet of Things: Privacy and Security in a Connected World, found that less than 10,000 households can produce 150 million distinct data points daily. And that number only reflects residential use. Enterprise businesses generate their own endless amounts of data

from a multitude of sensors, and in the security departments, this includes access control, video surveillance, analytics-based video applications and much more.

The Danger of Cybercrime

In 2016, the WannaCry ransomware attack infected more than 300,000 computers around the world. Frighteningly, the virus was spread by something as low-tech as an email. Britain's National Health Services was caught up in the attack. As a result, surgeries were canceled, staff reverted to pen and paper and only emergency patients could be treated.

The most well-known example of a cyberattack on critical infrastructure was the attack on the Ukranian power grid in December 2015 when 250,000 homes lost power as a result. Accessing the systems controlling the plant's circuit breakers did not require two-factor authentication, thus providing a security breach for the attackers to exploit with stolen credentials.

According to Kaspersky Lab research, the percentage of industrial computers under attack grew from 17 percent in July 2016 to more than 24 percent in December 2016. The top three sources of infection were the internet, USBs and email attachments.

A spear-phishing email was the technique used in an attack on a German steel mill in 2014. Here, the attackers gained access to the plant's network through an infected email attachment. The success of these non-complex methods would indicate low levels of awareness about how cyberattacks are carried out.

In a survey of nearly 600 utility, energy and manufacturing organizations, only half of the

companies had a dedicated IT security program. A hacker waits an average of 146 days from having penetrated a system before they strike; therefore, regular assessments give end users the opportunity to root out penetrations before they strike.

The dangers of cybercriminals are genuine. Last year, Kaspersky Lab discovered a ring of hackers called the Carbanak gang, where it was reported the ring had stolen more than $1 billion from financial institutions around the globe.

Hacks also can have dire economic impacts. For example, a possible hack that could trigger a blackout in North America is estimated to leave 93 million people without power and cost insurers anywhere from $21 billion to $71 billion in damages.

In a report by Cisco Cybersecurity in 2017, 35 percent of chief information security officers (CISOs) and security operations professionals said they see thousands of daily cyber threats, but only 56 percent are investigated.

> The WannaCry ransomware attack infected more than 300,000 computers around the world and was spread by something as low-tech as an email.

These numbers and facts only scratch the surface of incidents occurring around the globe that have the potential to wreak havoc on an organization and its valuable information. When a breach occurs, each organization must take steps to learn from the

outcome of other incidents and work toward strengthening the protocols in place for protecting breaches in the future. This starts with identifying how cybersecurity is handled at the basic level.

Who Is Responsible for Cybersecurity?

So now that we've identified and discussed IoT security and how the interconnectivity of devices can result in a greater risk of cyber threats and attacks, the question remains: Who is responsible for keeping data safe? With many players involved in the operation and maintenance of security devices, the uncertainy of this question is understandable.

According to a report from Radware, a provider of application delivery and cybersecurity solutions, there was no clear consensus among security executives when asked who is responsible for IoT security. Thirty-five percent of respondents placed responsibility on the organization managing the network, 34 percent said the manufacturer and 21 percent chose the consumers using the devices as being primarily responsible. The results demonstrate the answer: everyone.

Cybersecurity must become and remain top of mind for the organization, the manufacturer and the user. It's not surprising that the majority of people polled chose the organization as the main stakeholder for IoT responsibility; after all, if a company is managing a network, one would expect it to protect the network as well. This can be done by adapting user-centric design with scalability, tactical data storage and access with appropriate identification and security features (for example, the use of multi-level authentication through biometrics in access control). Organizations must also use their IT teams to strengthen the overall cybersecurity of the IoT by keeping up with the latest software updates, following proper data-safety protocols and practicing vulnerability testing.

Organizations must use their IT teams to strengthen the overall cybersecurity of the IoT by keeping up with the latest software updates, following proper data-safety protocols and practicing vulnerability testing.

Manufacturers that provide IoT-enabled devices as part of a security systems must be fully knowledgeable of the risks involved and effectively communicate them to the integrators or end users. Providing the education and dedication necessary for protecting users of its equipment makes a manufacturer more trustworthy and understanding in the eyes of an end user. Ensuring encryption between devices is a key step that manufacturers can take to work toward achieving complete protection in the IoT.

Despite the protection delivered by the organization and manufacturer, there's always the option for IoT security to be enhanced or possibly even diminished by the individual user. It's critical that best practices for data protection are in place every time an individual uses a device that is connected to the network. These include disabling default credentials, proper password etiquette, safe sharing of sensitive information and the instinct to avoid any suspicious activity or requests.

The best way to clear up the general misunderstanding about IoT security responsibility is to emphasize that every contributor to the development and use of an IoT-enabled device plays an important role that cannot be dismissed. Despite the growing fear of threats to the IoT, the organization, manufacturer and user can work together and combine techniques to form a guarded and secure system.

Best Practices for Protecting Data

In addition to the organizational level, it's critical to establish best practices for protecting data across all levels of a security installation. Here, we've outlined five ways to ensure data is safe:

Choosing the Right Equipment

One of the most obvious places to start is to choose equipment from reliable suppliers that have a knowledge and interest in cybersecurity and are focused on protecting your data. When your security system is designed from the ground up to protect against cyberattacks, naturally your organization will be in a much better place.

One way to establish whether the equipment can be trusted is to ask whether vulnerability-testing practices are in place. A security vulnerability in a product is a pattern of conditions in the design of the system that is unable to prevent an attack resulting. This will result in perversions of the system such as mishandling, deleting, altering or extracting data. Search for manufacturers that engage in this testing from the beginning, including the analysis of the type of cyberattacks that can potentially attack, break and disable a system.

Essentially, this form of testing puts the product through its paces, and once weaknesses are exposed, they can be patched up, and the cycle of attack-and-defense can take place again until eventually, a watertight ship is in place and ready for market. Testing is the critical discipline that helps identify where corrective measures need to be taken to rectify gaps in security. The more extensive an organization's security testing approaches are, the better are its chances of succeeding in an increasingly volatile technology landscape.

Evaluating the Weakest Link

The most obvious low-hanging fruit for hackers is to target people. Targeting people opens the door to the "weakest link" possibility that can uncover vulnerabilities, such as lack of authentication and encryption, and weak password storage that can allow hackers to gain access to systems. Notably, most hacks come down to human error whereby weak passwords, or clicking on contaminated email attachments, will expose an organization's security. Hackers have also been known to target contractors and simply wait until they go on site for scheduled maintenance with their infected laptops or mobile devices.

One way to help bolster defenses for individuals within an organization is to thoroughly establish procedures

and protocols for accessing critical data points, including ensuring multi-level authentication and communicating how this must be followed to protect the organization from outside threats. From a more colloquial standpoint, an organization's data is only as safe as how it's handled at the weakest point in the chain.

Keeping up with Regular Updates

Cyberattacks must also be prepared for long after the product is released to market. Manufacturers should prepare regular firmware updates to keep a product in the field readily prepared to address the latest critical bugs that can flood the market, such as the recent Meltdown and Specter bugs.

This is where continuous testing at the manufacturer level becomes critical, since as the protection of data becomes more robust, so do the methods by which this information is stolen or compromised by outside threats. Maintaining an open and transparent process for identifying potential holes in security is important to the overall security health of an organization and sets manufacturers apart.

Encryption

By encrypting before you send data and information to the cloud, it adds an extra cushion of control and power over that data. Not only does it provide an added defensive structure around a company's information, but it also adds peace of mind to the equation when relaying this data to the cloud.

Diligence

How can we best protect against the darker side of an increasingly connected world? By being open and transparent in exposing and reporting vulnerabilities. The best way to avoid attacks is to keep systems up to date, change passwords regularly, provide employee training and be diligent in safeguarding facilities through firewalls and following best practices in network maintenance. Keeping up with security updates allows us to make the most of the new technologies available today and into the future.

We can best protect against the darker side of an increasingly connected world by being open and transparent in exposing and reporting vulnerabilities.

With cybersecurity, you must act every week. It is not something where you can say, "We're safe, we're secure and let's forget about it." For manufacturers, every time a product is released, you must focus your mindset on cybersecurity from more reactive to more proactive, thinking consistently that an attack is coming and planning accordingly. ■ **Back to TOC**

Kim Loy (kimloy@vanderbiltindustries.com) is director of technology and communications for Vanderbilt Industries (vanderbiltindustries.com).

Search the SIA Membership Directory

The U.S. government is aware of ongoing threats and expends significant resources combating them, but they need assistance from their commercial supply chain community partners.

Leveling Up in Cybersecurity

Why Cybersecurity Is More Important Than Ever for Security Systems Integrators

Christine Lanning
Integrated Security Technologies

The 2018 Foreign Economic Espionage in Cyberspace report, issued by the National Counterintelligence and Security Center, makes it clear that economic and industrial espionage against the United States continues to be a serious threat. The report names China, Russia and Iran as the top three adversarial countries from a supply chain risk perspective.

The public is numb to popular media stories announcing how our adversaries have yet again exploited our cybersecurity vulnerabilities to steal proprietary commercial or defense industrial base intellectual property. The public perception of infiltrators who compromise our supply chain companies or take over command and control of our critical infrastructure systems is limited by understanding of

technology and the magnitude of the risk to our national economy.

We, as electronic security system integrators, don't have the luxury of ignoring this information. It is incumbent upon us as partners in the security community to do all that

is within our power to help defend against these espionage forces.

Industrial espionage is not a recent development. Foreign spies have been infiltrating our major technology centers for decades. As gaps in global technological advantage have narrowed, the efforts and stakes of this criminal enterprise have correspondingly risen. Our federal law enforcement partners have attributed hacking efforts during our 2016 election to the Russian government. In January 2018, Chinese hackers stole hundreds of gigabytes of data from a U.S. defense contractor. And while the data wasn't classified, it did contain information about a submarine supersonic anti-ship missile they had plans to complete by 2020. In 2017, three Chinese hackers working for a state-sponsored intelligence contractor were indicted for stealing intellectual property from three technology companies. This past March, an Iranian hacking group was indicted for stealing 31 terabytes of data from 144 American universities, totaling $3.4 billion in intellectual property. And then there is the Massachusetts-based American Superconductor, who nearly went out of business because the Chinese company who represented over three quarters of their business purchases refused to pay, stole their source code and then installed a pirated version of their software into the wind turbines that it sold. The U.S. government is aware of these ongoing threats and expends significant resources combating them, but they need assistance from their commercial

> For the last 20+ years, our industry has deployed electronic security systems into the IT environments of our customers without much of a thought to cybersecurity.

supply chain community partners. Here's what you can do to help.

The Parts of the Problem

It's only a matter of time before you or your customer get exploited and have your data corrupted, information stolen or systems disrupted. Maybe it's a ransomware attack on a hospital infant abduction system, and someone's child goes missing. Maybe it's a U.S. military base that allows someone with a fake credential and ill intentions in the gate because no one could accurately verify the person's identity because the system is compromised by a denial of service attack. Maybe your community's critical infrastructure utility system goes down because a security systems integrator left a backdoor default password open on a piece of substation equipment, allowing a criminal a way in and providing a platform for them to launch their control system attack.

For the last 20+ years, our industry has deployed electronic security systems into the IT environments of our customers without much of a thought to cybersecurity. Strong passwords? Takes too much time and too difficult to manage, they say. Encryption? Slows the system down. Device certificates? Too expensive. Standards-based installation? Proprietary systems keep our customers coming back to us.

With access control systems (ACS), we've been using the same Weigand communication protocol since the early 1980s. The Wiegand protocol connects card readers to ACS door controllers and has never been updated. It's widely known that readers are easily and continually hacked using very inexpensive replay attack tools – this is due to the lack of encryption

in the Weigand protocol. Similar copying vulnerabilities are present in the old 125khz proximity cards too, yet companies continue to install systems with these openly exploitable vulnerabilities. In 2012, the Security Industry Association (SIA) began developing a new protocol called open supervised device protocol (OSDP). This protocol is considerably more secure because is supports high-end encryption, and it is available across a broad spectrum of ACS manufacturers, yet there remains a lag in adoption, partly because customers haven't budgeted for system replacement. As an industry, we didn't tell them about our shared "problems" early enough, and in truth there are still many integrators that don't know about the advantages of OSDP.

To those issues, let's add the growing prevalence of Internet of Things (IoT) connected devices. Our industry continues to install IP devices like cameras, intercoms, speakers, microphones and alarm systems, ignoring standard cybersecurity practices and procedures. A 2015 Computerworld article warned that 100 percent of IoT home security systems that they tested failed against routine brute force types of attacks. Using the popular website SHODAN.io, today you can view over 200,000 security cameras across the globe that are still using their factory default passwords, evidence of a lackadaisical deployment practice. You can peer into people's homes and private businesses all because the installers didn't take the time to change the default passwords, and the customers didn't know to ask them about it. Oh, and if you think just changing the password solves everything, think again. A six-character password can be hacked using a brute force library attack in .02 seconds.

Why do systems integrators continue installing insecure systems? We have a duty and an obligation to protect the systems we deploy to make sure we aren't contributing to the problem. I've heard many integrators argue that customers aren't asking for cyber-hardened systems, or that they don't have the budget for pay for the extra security configuration work that it takes to install and monitor these devices properly. We have to do better as an industry than just waiting for customers to ask. We owe it to our customers to educate them about why cyber-hardened security systems are necessary and not just a luxury.

We have to do better as an industry than just waiting for customers to ask. We owe it to our customers to educate them about why cyber-hardened security systems are necessary and not just a luxury.

Awareness Is Key

The first thing a security systems integrator can do is educate

themselves. The good news is that there are a lot of great resources out there.

PSA Security (PSA) is the world's largest systems integrator cooperative made up of the most progressive security and audio-visual systems integrators in North America. Its mission is to empower its owners to become the most successful systems integrators in the markets they serve. As a part of that mission, PSA has developed a cybersecurity committee, a cyber advisory board and cyber solutions partners. SIA, PSA and ISC Security Events partnered to host the first-ever Cyber:Secured: Forum in June 2018; the conference discussed cyber-hardening of security systems, cyber standards and global cybercrime.

The PSA cybersecurity program provides educational programs and resources to integrators to assist them in navigating cybersecurity policies, processes and solutions ; the program website has a host of resources, including a cybersecurity playbook, information security small business fundamentals and a white paper on cyber risk.

Not a PSA Security owner or member? There are several federal agencies in the market to help your businesses with your cybersecurity, and they have a vested interest in doing so.

The U.S. Department of Homeland Security's (DHS') Office of Infrastructure Protection is dedicated to leading "the national effort to secure critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community." The office does this through risk management,

education, regulation, coordination, operational support, outreach and conducting site surveys.

In accordance with the National Infrastructure Protection Plan, DHS has classified critical infrastructure into 16 sectors whose assets, systems and networks – whether physical or virtual – are considered so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety or any combination thereof. Some of the more obvious sectors cover energy, communications, nuclear reactors and nuclear materials. Water and wastewater as well as health care are broken out with specific recommendations for their physical security. There are other obvious sectors, but many security integrators that I've met don't know there's a special subsection for commercial facilities like hotels and condominiums, a sector that consumes a lot of security technology

Two of the more important DHS programs are education/free training and site surveys.

The Critical Infrastructure Learning Series "provides one-hour, web-based seminars conducted by critical infrastructure experts on the tools, trends, issues and best practices for infrastructure security and resilience". The series also offers instructor-led classes all over the country on a wide variety of topics, including active shooter, counter-improvised explosive device (IED) training and awareness, cybersecurity, chemical terrorism, retail security awareness and protecting critical infrastructure against insider threats.

Several of these courses are also listed on the Federal Emergency Management Agency website along with others, such as a workplace security awareness course, a surveillance awareness course and a protecting critical infrastructure course.

DHS has a free survey tool – the Infrastructure Survey Tool – created

by its protective security advisors; this tool is requested by a facility and designed to identify facilities' physical security, security forces, security management, information sharing, protective measures and dependencies related to preparedness, mitigation, response, resilience and recovery. The tool will also find security gaps in addition to creating protective and resilience measures indices that can be compared to similar facilities.

The FBI also has several programs available. As the lead agency for investigating cyberattacks, the FBI has developed a website – the Internet Crime Complaint Center – that allows users to report internet crimes, including ransomware, business email compromise, phishing, tech support fraud, data breaches and extortion. Users can fill out an online form, and it goes directly to the FBI for review.

The FBI also has a program called InfraGard, which brings together the FBI and the private sector to exchange information and promote learning opportunities relevant to the protection of critical infrastructure. There are 82 InfraGard chapters nationally; membership is free, but applicants must agree to a cursory background check.

As a part of its community outreach the FBI has established a Citizen's Academy to foster a greater understanding of the FBI's role in the community for business, civic and community leaders. These academies are usually held one night per week for eight to ten weeks, exposing students to the various investigative inner workings of the FBI.

If you don't have time to participate in your local area groups, at least get to know your local federal agents from DHS and the FBI. Along with the wealth

of information available to you as a systems integrator, it's always best to have a relationship with them before something bad happens and you need to engage their services.

Regulation

Still not convinced of the importance of this issue? In 2017, the U.S. Department of Defense (DOD), fed up with its industrial base's slow adoption of sound cybersecurity practices, augmented the Defense Federal Acquisition Regulations (DFARs) to force companies to comply with cybersecurity standards in their own businesses. DFARS regulation 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting details how a contractor is supposed to provide adequate security for information systems and how to report a cybersecurity incident.

Now, contractors doing business with DOD must attest to their compliance with the National Institute of Standards and Technology's (NIST's) Special Publication (SP) 800-171 standards to meet the contractual rules of the DFARs clause. The NIST 800-171 standards are a subset of basic security controls for information systems derived from the broader NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations. The idea is to protect the processing, storage and transmission of controlled unclassified information (CUI). CUI information that is sensitive and relevant to the interests of the U.S., including facility security

> The bottom line is if you don't take cybersecurity seriously, you can expect to lose contracts. The Pentagon declared, "if your systems aren't cyber-hardened, you won't be doing business with us."

Systems Addressed by NIST 800-171 Controls

1. **Access Control** (Who is authorized to view this data?)
2. **Awareness and Training** (Are people properly instructed in how to treat this info?)
3. **Audit and Accountability** (Are records kept of authorized and unauthorized access? Can violators be identified?)
4. **Configuration Management** (How are your networks and safety protocols built and documented?)
5. **Identification and Authentication** (What users are approved to access CUI and how are they verified prior to granting them access?)
6. **Incident Response** (What's the process if a breach or security threat occurs, including proper notification?)
7. **Maintenance** (What timeline exists for routine maintenance, and who is responsible?)
8. **Media Protection** (How are electronic and hard copy records and backups safely stored? Who has access?)
9. **Physical Protection** (Who has access to systems, equipment and storage environments?)
10. **Personnel Security** (How are employees screened prior to granting them access to CUI?)
11. **Risk Assessment** (Are defenses tested in simulations? Are operations or individuals verified regularly?)
12. **Security Assessment** (Are processes and procedures still effective? Are improvements needed?)
13. **System and Communications Protection** (Is information regularly monitored and controlled at key internal and external transmission points?)
14. **System and Information Integrity** (How quickly are possible threats detected, identified and corrected?)

Information provided by Kelser Technology Forward

drawings and device or network configuration information.

Does your company do business with DOD? Do you want that business to continue after 2017? Subcontracting does not exempt you from the DFARS clause, either – the clause flows down to subcontractors in cases where CUI passed to the subcontractor. The bottom line is if you don't take cybersecurity seriously, you can expect to lose contracts. The Pentagon declared, "if your systems aren't cyber-hardened, you won't be doing business with us."

The Pentagon isn't the only agency considering cyber-hardened company selection. There has also been some talk about including security related to cyber hardening as a "fourth pillar" in the acquisition process, along with cost, schedule and past performance, which will force government contractors to consider their internal IT practices as well as their deployment of systems. They want your assurance that your own IT systems will provide an acceptable level of security. And having these regulations forced on government contractors will make those contractors more attractive to all customers seeking a more secure system.

Conclusion

In 2015, when the industry started paying attention, you were likely just procrastinating with cybersecurity, unsure of what the future would bring. In 2018, that same attitude probably makes you negligent. Cybersecurity negligence in our people, processes and products is no longer being tolerated in our client industries. Cybersecurity negligence is something our customers, our communities and our nation can no longer afford from their supply chains.

Maybe Acme's Auto Body Shop doesn't care about a fully encrypted, cyber-hardened security system at its facility, but it's clear that the critical infrastructure sectors do. Supply chain scrutiny is increasing across the energy, health care, finance, transportation and food supply sectors. New regulations surrounding the supply chain companies in all sectors are being discussed, and many are considering adopting NIST 800-171 until they have time to build more sector-specific cybersecurity control sets. Expect cybersecurity clauses to appear in your next round of commercial negotiated contracts if you work with regulated industry sectors. If you want to continue to do business with companies in these sectors you're going to have to prioritize the cybersecurity posture of your organization.

New regulations surrounding the supply chain companies in all sectors are being discussed, and many are considering adopting NIST 800-171 until they have time to build more sector-specific cybersecurity control sets.

The writing isn't figuratively on the wall any longer; it's written contractually in the Defense Acquisition Regulation System. Cybersecurity vulnerabilities can't be ignored. You'll have to cover your liabilities with insurance, and the less you know about and mitigate those vulnerabilities, the more you're going to pay. Continued negligence could potentially force you from the industry as your cyber-aware competitor's offerings evolve beyond your own.

Remember Blockbuster, who didn't want to send DVDs through the mail and missed out on the streaming video services that Netflix envisioned? Remember Borders Books scoffing at the Amazon threat? Recall how BlackBerry held onto its proprietary systems and insisted that no one wanted touch screen technology on their phones? Look at the taxi companies fighting the next evolution of ride sharing. These are all examples of failure to evolve in the era of digital transformation. Security system integrators are at a critical point at which their executive planning decisions must be made with cybersecurity awareness at the top of their agendas. People, processes and products must all be assessed and aligned with sound cybersecurity practices. Any decisions made without an eye towards the cybersecurity threats that we are experiencing daily might as well be made with the flip of a coin. For some, perhaps taking that chance is better than admitting that they're completely blind. ■ **Back to TOC**

Christine Lanning, MSIS, PSP, (christine@istechs.net) is president of Integrated Security Technologies, Inc. (istechs.net).

Search the SIA Membership Directory

An increasing number of periphery devices that were once analog-based and largely segregated from other IT systems have transitioned to IP and are becoming a greater cybersecurity threat.

How Technology and Risk Are Changing the Banking Market Today and for the Future

Courtney Mamuscia
Verint

The banking environment faces a multitude of risks, which are evolving and changing daily. Fraud, at the top of the list, leads to significant losses if not controlled, and today more than ever, banks are laser-focused on minimizing fraud attempts and must adopt a proactive approach to stay one step ahead.

Most banks have invested heavily in physical and network security to protect against traditional threats, but today greater threats loom on the horizon in the form of the Internet of Things (IoT) and the increasing number of periphery devices residing on the corporate network. Such devices include video surveillance, identity and access management and other physical security systems that are critical to the day-to-day operations of financial services firms.

These technologies, which were once analog-based and largely segregated from other IT systems, have transitioned to IP and are becoming a greater cybersecurity threat themselves. And with the proliferation of the IoT, a significant portion of which

is comprised of security sensors, this problem is only going to grow. In fact, according to research firm Gartner, more than 8 billion connected devices were in use in 2017 and that is forecast to grow to more than 20 billion by 2020.

What Can Be Done?

The problem for most banks is that they already have thousands of cameras deployed throughout their various corporate offices and branches, which makes trying to address cyber vulnerabilities a tremendous challenge. Let's take the typical branch surveillance deployment, for example. There is usually a mix of both existing analog cameras and IP cameras, along with an encoder, a network switch and a network video recorder (NVR) that is connected to the network. The NVR, switch, encoder and IP cameras all have firmware that may need to be updated to mitigate potential cyber risks, and most of them also typically have usernames and passwords that could be exploited by hackers. Updating these devices individually on a site-by-site basis presents a logistical nightmare, which makes having some type of centralized management utility a must.

> Numerous suppliers now offer leasing programs for their equipment and software, shifting the cost to an operational expenditure.

Aside from deploying centralized management, other steps that security managers at financial institutions should take to mitigate cyber threats to their physical security systems include:

- **Regular Technology Refresh Cycles:** Although many banks today replace computers and

other IT hardware every three to five years, the same cannot be said of their security equipment. Security devices, like other technologies, are changing very quickly, which means vendors are phasing out certain pieces of equipment more quickly and will eventually stop supporting them. Getting buy-in for a technology refresh can be challenging, but unlike the days where these systems had to be purchased outright, numerous suppliers now offer leasing programs for their equipment and software, shifting the cost to an operational expenditure and placing the onus for maintenance back onto the vendor and/or integrator.

- **Check and Perform Firmware Updates:** Manufacturers today are routinely updating their products to ensure they're protected against the latest threats. Unfortunately, many organizations are still woefully lagging when it comes to applying patches to impacted devices.
- **Practice Good Password Hygiene:** Network security experts have written at length in recent years about the need for organizations and their employees to leverage strong passwords, and the same thing can be said with regards to periphery devices, such as cameras and NVRs. Often, however, the passwords being used on these devices are still the default ones that came with them from the manufacturer or were changed to simple passwords like "123456" or "password."
- **Leverage MAC Access Control Lists (ACLs):** Many people

within IT security departments at financial institutions are concerned about the potential of an unauthorized user gaining access to a camera switch at a bank branch, plugging in a laptop and infiltrating the network or introducing a vulnerability to periphery devices themselves. ACLs allow end users to detect the MAC address of an IP camera and, should it be unplugged, subsequently block any other device from connecting to it.

Cybersecurity is only one critical challenge on the minds of today's banking leaders. To stay up to speed with a constantly shifting risk landscape and progressing threats, financial institutions must not only plan for today, but also look ahead to ensure the most innovative technologies and solutions are leveraged in the constant fight against fraud. As new trends and strategies emerge, security leaders should stay prepared and continuously work to gather as much data and intelligence as possible to modernize, simplify and automate their business.

Moving forward, the common goals of most financial organizations – satisfactory customer engagement, enhanced security and fraud reduction – will be significantly affected by these factors:

Big Data and Analytics

It has become clear that for financial organizations to predict and identify threats in real time, actionable, intelligent data analysis that links cyber and physical security must take place to present a unified risk scenario to the appropriate analysts and operators. Tomorrow's analytic applications will propel increased situational awareness and provide instant notifications to facilitate immediate action.

Automation and Modernization

Solutions of the future must allow security teams to dedicate time and effort to relevant tasks and

efficient responses, while leaving certain operations, such as firmware updates and camera verification, up to automation. Modernized processes will need to take advantage of prominent trends, including the IoT and the cloud, while elevating the customer experience and overall loyalty.

It's not just the monetary loss that banks need to be concerned about – there is also a threat to the brand, customer trust and employee safety.

Advanced Investigative Tools

Security systems will continue to develop to support streamlined and simplified investigations. Biometrics are poised to impact the financial market tremendously, as technologies such as facial recognition and voice analysis create the potential for banks and credit unions to strengthen identification processes and track fraudsters.

Artificial Intelligence

Financial organizations should consider leveraging the latest in artificial intelligence and advanced analytics to help unlock the potential of automation and innovation as it relates to customer service. For example, intelligent systems can analyze customer activity by performing accurate people counting, tracking customer behavior (such as dwell times and wait times) and evaluating branch action. By leveraging this information, institutions can make informed decisions that can impact efficiency and safety and inevitably enhance customer satisfaction.

Banks around the globe face a new risk paradigm almost daily and require innovative strategies and tools to strengthen the security of valuable data and assets. The fact is that it's not just the monetary loss that these businesses need to be concerned about – there is also a threat to the brand, customer trust and employee safety.

The practice of security – both cyber and physical – is a critical component of a bank's organizational structure. It helps secure the branch footprint, alleviates risk, ensures operational compliance and improves fraud investigations. As we move through the remainder of the year, we will continue to see Big Data analysis, video analytics, cybersecurity and IoT-powered devices allow for the collection of myriad data points across systems, services and devices and also open doors to additional risk that must be managed. The banks prepared to investigate threats in a more proactive manner and generate actionable intelligence from collected data will be the ones best positioned to achieve their strategic intelligence and business objectives. ■ **Back to TOC**

Courtney Mamuscia is director of marketing for Verint.

Search the SIA Membership Directory

If you are a woman entrepreneur considering starting a business or an established women-owned small business looking to do business with the government, the best starting point is the U.S. Small Business Administration's guide.

A Guide to Doing Business With the Federal Government for Women in the Security Industry

Lynn A. de Seve
GSA Schedules, Inc.

In 2016, the U.S. Department of Defense, the General Service Administration (GSA) and NASA adopted a final ruling amending the Federal Acquisition Regulation (FAR) to implement regulatory changes made by the U.S. Small Business Administration (SBA) providing authority to award set-asides and sole source contracts to economically disadvantaged women-owned small businesses (EDWOSB) per FAR 52.219-29 and women-owned small businesses (WOSB) per FAR 52.219-30. The rule provides a much-needed resource to federal agencies to meet the mandated 5 percent of all prime and subcontract contracts for small women-owned businesses.

The rule provides that EDWOSBs and WOSBs may receive set-asides and sole source awards in

industries designated by the SBA and North American Industry Classification System (NAICS) codes as "underrepresented" by women. Under the rule, an agency may make a sole source award in an appropriate industry where:

1) the contracting officer does not have a reasonable expectation that two or more EDWOSBs/WOSBs will submit offers,
2) the anticipated award price (including options) will not exceed $6.5 million for manufacturing contracts and $4 million for other contracts,
3) the EDWOSB/WOSB is responsible and
4) in the estimation of the contracting officer, the award can be made at a fair and reasonable price.

The rule allows the SBA or the contracting officer to protest the prospective awardee's EDWOSB or WOSB status. A competitor, however, cannot file a formal EDWOSB or WOSB status protests in regards to a sole source award.

For women-owned businesses in the security industry, this is good news. Qualifying NAICS Codes for WOSB include, for example: 561621 – security system services (except locksmiths); 561622 – locksmiths; 561611 – investigation services; 561612 – scurity guards and patrol services; 561990 – support services; 541990 – all other professional, scientific and technical services; 541690 – other scientific and technical consulting services; 541330 – engineering; 334512 – automatic environmental controls

The Women Business Center has a nationwide network of over 100 educational centers specifically designated to help women entrepreneurs.

(physical access control); 334390 – other communication equipment manufacturing (video management systems); and 541511, 541512, 541513 and 541519 – computer programming, design, management and other related services. These are just some of the categories related to the security industry that may apply to your business as you register your company for doing business with the federal government at the System for Award Management (SAM), a mandatory action.

If you are a woman entrepreneur considering starting a business or an established women-owned small business looking to do business with the government, the best starting point is the SBA's guide.

SBA's Office of Women's Business Ownership (OWBO) provides a wealth of information and assistance. OWBO was established to help women business owners with various programs coordinated by district SBA offices. Every state has an office, and some of the larger states have regional offices. OWBO oversees the Women Business Center, which has a nationwide network of over 100 educational centers specifically designated to help women entrepreneurs. Learn how to connect with your local SBA district and get resources in your area. The center offers training and counseling in several languages with a strong focus to assist in overcoming economic and social disadvantages. Other resources include local assistance with SBA loan programs and a lender match tool.

More established women-owned businesses may want to consider doing business with the federal government. The SBA has established a women-owned small business federal contracting program. Understanding and complying with eligibility requirements to be considered as a WOSB or EDWOSB under this program

is essential to success and assuring compliance for potential orders. Without this step, your company could be considered ineligible for a woman-owned set-aside or sole source at award. As previously noted, there is a 5% contracting goal for women. Certain government contracts have limited competition and restrictions to specifically benefit EDWOSB and WOSB.

Per Title 13 Part 127 Subpart B of the Code of Federal Regulations, a company must meet the following requirements to be considered a WOSB:

- Be a small business
- Be 51% owned and controlled by women who are U.S. citizens
- Have women manage the day-to-day operations and make long-term decisions

To be consider as an EDWOSB, a company must:

- Meet all the requirements of WOSB
- Be owned and controlled by one or more women each with a personal net worth less than $750,000
- Be owned and controlled by one or more women each with $350,000 or less adjusted gross income averaged over the last three years
- Be owned or controlled by one or more women each with $6,000,000 or less in personal assets

WOSBs Must Certify at certify.sba.gov

A company may self-certify or use a third-party certifier. You must first register your company with SAM at sam.gov. Be prepared to provide specific company and staff information and attest to various certifications and representations for your company. Then you must upload additional required documentation into the WOSB repository; this checklist can help you prepare for the SBA WOSB self-certification. The checklist will detail the

appropriate documentation needed to be submitted for certification of your company's eligibility, whether a WOSB or an EDWOSB, including financial information and, if applying for EDWOSB, a narrative of very specific details on incidents of discrimination socially and economically as a woman owned business.

Seek opportunities with prime contractors required to set aside business for women-owned small businesses.

There are four organizations approved by the SBA to provide third-party WOSB certifications:

- EL Paso Hispanic Chamber of Commerce
- National Women Business Owners Corporation
- U.S. Women's Chamber of Commerce
- Women Business Enterprise National Council

Certification from third-party organizations, although not required, can be very beneficial to verifying your WOSB status. Both government agencies and other prime contractors or Fortune 500 companies looking to certify their partners may give strong consideration with WOSB certifications are presented. SBA does not send certification letters.

Registration of your company in SAM, consulting with SBA, taking advantage of the unique eligibility and special concessions for WOSB and EDWOSB may help your women-owned security business obtain new customers. Seek opportunities with prime contractors required to set aside business for women-owned small businesses. The WOSB program also applies to the GSA Multiple Award Schedule contract, which offers a streamlined contracting vehicle for federal, state and local government, universities and other public institutions for purchasing security products and services under GSA Schedule Contract 84. This program contains the products and services deemed eligible per the NAICS codes for WOSB set-asides and sole source awards, as previously noted. A third-party certification as a WOSB may be a great marketing advantage.

Ladies, let's take advantage of the resources provided to help us succeed in business through the SBA and other advocacies for women. Consider these unique opportunities to expand our businesses as available to us for selling products and services to the federal government under a program offered to assist WOSBs with a focus applied to our industry. Be aware that, in addition to the SBA WOSB program and federal set-asides, the security industry is encouraging growth of diversity. For further discussion, additional support and encouragement is offered through groups such as the Security Industry Association's Women in Security Forum. ■ **Back to TOC**

Lynn de Séve (lynn@gsa-schedules.com) is president of GSA Schedules, Inc. (gsa-schedules.com).

We must recognize the reality that video in which a person can be identified is also considered personal data and is therefore subject to GDPR guidelines and requirements.

Security Organizations' Dual Responsibility Under GDPR

GDPR affects security technologies like video surveillance systems. Here's what you need to know to improve your GDPR compliance.

Lora Wilson
Axis Communications, Inc.

Since the General Data Protection Regulation (GDPR) was implemented on May 25, much of the information has been focused on how organizations can – and must – approach their data practices to not only become compliant but also maintain that compliance.

GDPR is a regulation set forth to protect personal data and ensure the privacy of individuals within the European Union (EU), which is deemed to be a fundamental human right. The primary driver behind the regulation is to give individuals greater control over their personal data and how it is used. Despite its roots in the EU, GDPR also addresses the collection or storage of personal data from any EU citizen, as well as the export of data outside the region. Therefore, given the scope of GDPR, compliance is a global concern.

Because cybersecurity was a main driver behind GDPR, one of its mandates is that in the event that a data breach occurs, companies that collect personal data are mandated to report it in to the supervisory authority within 72 hours. Failure to comply with

this regulation could result in penalties equaling 4 percent of a company's global annual revenues or 20 million euros, whichever is greater.

Given the importance of individuals' privacy and the potential penalties for non-compliance, these are important discussions; however, this focus is not enough for those of us in the security industry, who have a dual responsibility under GDPR. Why is that?

In practical terms of protecting individual privacy, GDPR places much of the responsibility and obligation on businesses and other organizations that deal with personal data. One of the key features of the new regulation is that those who are being monitored need to be fully informed about what data is being held on them and how it is being used.

Under GDPR, this "personal data" is defined very broadly as "any information relating to an identified or identifiable natural person," referred to as the "data subject." Naturally, the first types of personal data that come to mind are the classic examples such as name, physical address, phone number and email address, all of which meet the criteria. But these are only starting points, as the range of personal data types is expansive, encompassing more than simply text-based data.

As security professionals, we must recognize the reality that video in which a person can be identified is also considered personal data and is therefore subject to GDPR guidelines and requirements. Therefore, as organizations, we need to determine how best to become compliant with how we handle customer and employee data, including surveillance video. This dual responsibility must come into play when we consider how we design and operate security systems and collect video data through surveillance, including how we store and manage that video data after collection.

To do so, it is important to explore how many of the steps organizations must take to become

GDPR compliant are also necessary to ensure that video surveillance data is compliant as well. These steps surveillance operators must take – and how they can be applied to collected video – are outlined below.

Administration

In general, the first step in ensuring GDPR compliance is to choose an administrator and record data processing activities. As an organization seeking to become GDPR compliant, it is essential to have a person on staff – known as a data processing officer – who will ultimately be responsible for data integrity. Each company providing video surveillance must choose an administrator.

In a security environment, choosing this administrator allows for an open way to publicly identify the person who is responsible for data collected from the surveillance systems and provide that detail to anyone who is monitored by video upon their request. In doing so, it is key to also make the name of this data processing officer available to every person who requests data as prescribed under GDPR.

Every organization should also have a procedure in place for when an individual chooses to exercise their right of access to personal data or request its deletion, which allows them to stay within the monthlong window within which GDPR requires them to comply with these requests. When making such a request, it is reasonable to expect an individual to provide adequate information in order to locate this data – for example, an approximate timeframe, and the location where the footage was captured.

Documentation

GDPR also recommends that record of processing activities (ROPA)

documentation be maintained and the following information be made available upon request:

- Category of individuals that processed personal data relates to
- Purpose for which collected data is used
- Whether personal data will be transferred (to whom and for what reason)
- How long personal data will be stored
- Description of technical and organizational measures to ensure privacy

According to GDPR, administrators should take all appropriate measures to provide this information concerning the processing of their data by surveillance systems to monitored individuals in a brief, transparent, comprehensible and easily accessible manner.

ROPA documentation must also include a risk assessment for individuals' rights and freedoms and planned measures to address these risks, which include safeguards and mechanisms to ensure the protection of personal data and compliance with GDPR. This should take into account the rights and legitimate interests of individuals and other affected persons.

In a surveillance environment, these items are equally important. Focusing for a moment on purpose and extent of surveillance, it must be clear why and how much video is being collected, and for what reason. One thing to discuss with potential solution providers is the concept of privacy by design and "GDPR-ready" product features. In evaluating solutions, organizations should look for those that will help them more easily become GDPR compliant. An example would be technology supporting defined view of a specific perimeter. By leveraging solutions to define the perimeter, organizations adhere to

GDPR in that they can more easily specify the extent of video surveillance.

Data Processing Inventory Assessment (DPIA)

Once an administrator has been chosen and ROPA documentation is complete, a DPIA is required for cases of "extensive systematic monitoring of publicly accessible premises."

This requires specifying in writing why and for what purposes the camera system is recording. For example, a city needs to manage electrical and water utility stations and must ensure the utilities provide residents with dependable service. Therefore, the perimeter of these utility stations must be protected against crime and theft. Under GDPR, the city can specify that the surveillance is provided for this purpose. Another example would be to ensure the safety of citizens during public events, as surveillance video may be used by the police to provide real-time situational awareness for officers in the field. In this case, it can be specified, in accordance with GDPR guidelines, that video is being collected to support public safety.

This information directly correlates to ROPA documentation, so again we can see the connection between becoming compliant as an organization overall, as well as ensuring compliance for GDPR with information and data collected in a surveillance environment.

Data Security

Cybersecurity has been a major topic within the security industry for some years now. The importance of a surveillance system being cyber secure extends to compliance with GDPR, with tight control of video data being another key recommendation. It is vitally important when specifying a system that these critical measures are taken into account. The less data that is readily accessible to those outside the scope of an organization's video data management procedures, the less risk there is of becoming non-compliant. The same philosophy applies to data breaches; administrators must

report any leaks within 72 hours of notification.

To ensure GDPR compliance, companies should employ strong measures to prevent unauthorized access to the personal data they store, including video. The specific tools and tactics used by each company will be unique to the challenges they face. In all situations, however, companies must employ robust security controls, stay up to date with cybersecurity best practices and ensure they are working with trusted partners that provide secure hardware and software, as well as thorough aftercare. Therefore, organizations must work with security professionals and partners to better understand potential cybersecurity risks and talk about ways they can harden their systems to ensure GDPR compliance.

From a compliance perspective, the processes that must be put in place to ensure the "right to be forgotten" in an organization are very similar to those necessary to ensure a surveillance system is also in compliance. This requires taking a systematic approach to how video data is stored, transferred and deleted. These methodologies will ensure that if an individual requests his or her video footage be deleted, business systems and organizational structure will be in place to adhere to this request in an efficient manner. The concept of "right to be forgotten" is a significant part of the GDPR guidelines, and as we are just months into this new guideline, the impact on organizations and system operators after requests are submitted still remains to be seen.

Ultimately, it is the surveillance system user (i.e., data controller) who is responsible for GDPR compliance and safeguarding the rights of individuals whose personal data the user collects and processes.

End-to-End Compliance

It is important to consider the full scope of video surveillance. As a surveillance operator collecting video about living individuals, an organization will fall under the category of data controller and be held responsible for data management in accordance with GDPR. Anyone having access to video data, including subcontractors and hosted service providers, must meet requirements as well. These companies or individuals who have access to recorded video on behalf of an organization, such as hosting providers, fall under the category of data processors. In terms of company compliance, when reviewing contracts to ensure all companies comply in the same way as an organization has planned. In terms of surveillance, be sure to check that any persons or organizations who have access to video are also compliant and

that contractual relationships reflect these obligations.

Ultimately, it is the surveillance system user (i.e., data controller) who is responsible for GDPR compliance and safeguarding the rights of individuals whose personal data the user collects and processes. While the data controller has ultimate responsibility to follow GDPR, data privacy is a team effort. Remember: We are all in this together.

Therefore, for users of surveillance equipment, solutions and services, it is important to partner with suppliers that are committed to respecting and safeguarding individuals' privacy and protecting personal data. Users should also be able to rely on suppliers and vendors for the support and technical assistance necessary to facilitate GDPR compliance.

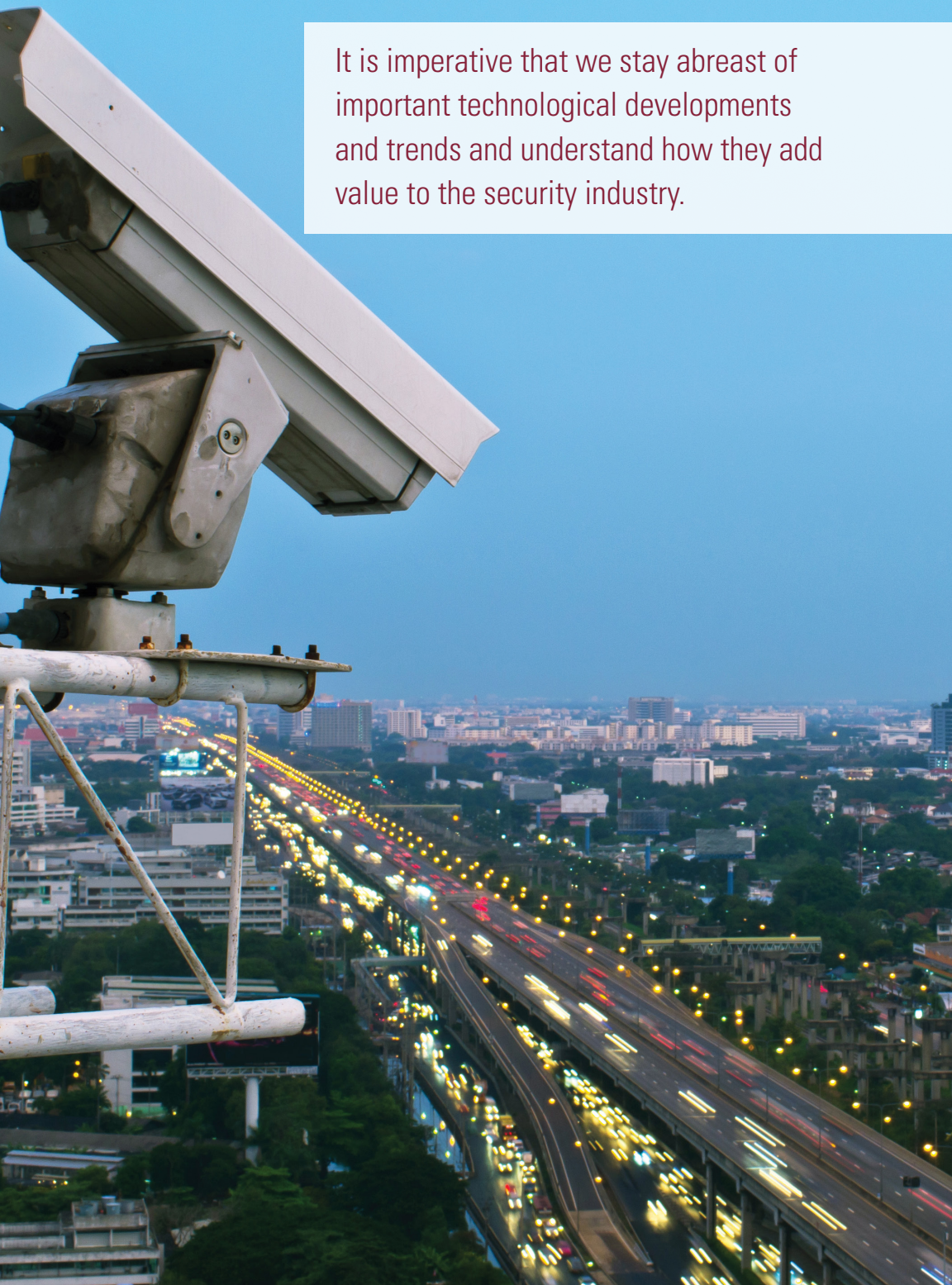
Due to its intent, the onset of GDPR is a positive one. It will allow data processors and controllers to use data in appropriate ways and have clear guidelines/procedures in place for data collection, management and surveillance. Many companies follow guidelines such as the UN Global Compact when it comes to sustainability and environmental responsibility. The UN Global Compact provides 10 clear principles to help guide companies in their sustainability efforts. GDPR provides similar clear direction to companies looking to protect individual privacy, a fundamental human right. ■

Back to TOC

Lora Wilson (lora.wilson@axis.com) is director of marketing for Axis Communications Inc. (axis.com).

Search the SIA Membership Directory

It is imperative that we stay abreast of important technological developments and trends and understand how they add value to the security industry.



Four Tech Trends Shaping Today's Video Surveillance Industry

Cloud-based solutions, big data, artificial intelligence and managed services all are poised to revolutionize the security industry.

Ann Ottinger
Geutebrück USA

It is an exciting time to be involved in the security industry. The pace of technological advancement is such that the rate of development seems to outpace even our most fantastical imaginings. Today, technologies are arriving swiftly, filling roles we never could have dreamed and maturing more quickly than ever.

With such swift innovation, however, it is imperative that we stay abreast of important technological developments and trends and understand how they add value to the security industry.

The Evolving Role of Cloud-Based Video Management System (VMS) Solutions

Remember the good old days of CDs and DVDs for your music and videos? Those days are long gone along with the stores and businesses who used to sell them. Today the majority of the world streams music and movies. We store and manage almost everything we do electronically in the cloud.

This is the same with the devices we carry and the computers we

use every day, which have become mostly user interface devices. The applications and software programs are largely subscription-based services managed, updated and maintained on cloud servers. Today when we need to replace a device, we log in and restore from the cloud. Cloud backup subscription services have been around for years and are growing because they leverage the shared cost of necessary hardware and the low cost of storage.

There is no debate that in the very near future, our industry will not be installing video management hardware with on-site video and data storage in the local server racks of end-user customers. Some manufacturers in our industry are already embracing this technology and developing the VMS solutions of the future. The obstacle of affordable and available bandwidth is quickly disappearing. The facts are that these clouds have already been built and that they are being widely used by every other industry. While some may argue that managing video is totally different, this trend is not going away, and our industry must embrace this or ignore it to our peril.

The Internet of Things (IoT), Managing Big Data and Cybersecurity

With each passing year, big data continues to proliferate, reaching every aspect of our lives. Data is collected and streaming from everything imaginable today thus the term IoT. From the phones we carry, to the cars we drive and the refrigerators which store our foods, data sensors are being used in our homes, at our schools, in

our businesses and industries and all across the cities of our country.

This gathering of information is scary to some and raises legitimate concerns over who has access to the data and how we secure it. Beyond the cybersecurity issues, there are important questions about how the collected data will be used and what we can do to protect our individual privacy.

There is also a proliferation of data analysis companies specializing in software designed to collect, analyze and generate meaningful reporting on this wealth of collected data. These companies understand that data is knowledge and the value of that knowledge can create measurable return on investment. Businesses and industry use collected data, too, as they continue to look for ways to become more productive and efficient and thus more competitive by producing more with less. In spite of this global trend, the video surveillance industry has generally been slow to realize the value in integrating their systems with this data.

The Role of Artificial Intelligence (AI) in Video Surveillance

There are many definitions for AI, and the term is thrown around these days for many things that are not actually AI. Many of the analytics used in video surveillance are being touted as AI when, in fact, they are heavily dependent on human intervention, monitoring and programming.

When examining the future of AI in video surveillance, I believe the industry should focus on the subset of AI called machine learning. In this area of AI, new technological advances in video analytics should actually learn and adapt accordingly to their assigned tasks, without the intervention of humans. Future video surveillance management software will include elements of this self-learning ability and will apply AI to the vast amounts of data they collect in addition to studying the video images themselves.

One example already being developed and deployed is predictive analytics, a basic function of AI machine learning. In this application of AI, the system learns over time and

determines the statistical probability of predetermined events. Basing these predictions on solid historical data and patterns, collected and measured, leading to similar events. Expect to see this technology become standard in the future.

Opportunities in Managed Services

Many who read this article may find humor in my stating that the security industry as a whole lags behind other industries in adopting proven technology and methodology. Many of the best technologies we use today in video surveillance were proven and used for many years in the consumer electronics or IT world before ever being adopted into our industry.

Managed services agreements (MSAs) are similar because they have been used in the IT world for as long as I can remember. Statistically, according to CompTIA's Buying Guide for Managed Services, 64 percent of organizations in 2016 were using some form of managed services. The study went on to say that the managed services market was expected to grow to $193 billion by 2020, a growth rate of 12.5 percent. Today MSAs in IT are being used by an estimated 80 percent of businesses and organizations

The leaders in the IT world realized long ago that it was easier to sell a managed services agreement that included all necessary hardware, software and support, which essentially amortized the expense over a 3- to 5-year term. For most organizations, budgeting an annual operational expense (opex) was easier than obtaining approvals for a large capital investment (capex). So why not apply the same strategy to video surveillance?

For most organizations, budgeting an annual operational expense (opex) was easier than obtaining approvals for a large capital investment (capex). So why not apply the same strategy to video surveillance?

A video surveillance system is just another information technology solution consisting of servers, switches and other network components that manages data. So why does our industry not embrace the MSA model, so overwhelmingly popular in other areas of the IT world?

As our industry continues to evolve into cloud-based management systems, intelligent solutions with AI machine learning and systems designed to manage and integrate big data with video images, managed services create the ideal business model. Like other untapped areas of our industry, offering an MSA program creates great opportunities for growth and creating a substantial recurring monthly revenue model for the video surveillance market. ■ **Back to TOC**

Ann Ottinger (ann.ottinger@geutebruckusa.com) is vice president of Geutebrück USA (geutebruckusa.com).

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:

S18: Spring 2018
F17: Fall 2017
S17: Spring 2017
F16: Fall 2016
S16: Spring 2016
F15: Fall 2015
S15: Spring 2015
F14: Fall 2014
S14: Spring 2014
W13: Winter 2013-14
J13: June 2013

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

Access Control/Identity Management

Modern Face Recognition Systems (S18)
Living the revolution as algorithms based on Deep Neural Networks (DNN) come to market
By Alexander Khanin, Vision Labs

More than Just a Silver Lining (S17)
Using the cloud for access control enhances scalability, availability, resiliency, flexibility and security
By Denis Hébert, Feenics

Walk this Way, Talk this Way (S17)
Combining gait analysis, voice recognition and other biometric identifiers provides a fraud-resistant security solution
By Maj. Gen. (ret.) Aharon Zeevi Farkash, FST Biometrics

A Matter of Trust (S17)
New digital identity technologies will increase security, functionality and convenience in many areas
By Stefan Widing, HID Global

By the Power of Ethernet (S17)
PoE gives smaller facilities more access control options
By Kerby Lecka, Security Door Controls

An Eye for Fraud (S17)
Iris recognition technology offers one of the most effective ways to prevent medical identity theft and false claims
By Jeff Kohler, Princeton Identity

Raising the Standards (F16)
Physical access control can benefit from adopting an IT-centric approach
By Scott Sieracki, Viscount Systems

In a Hand or a Face (F16)
Fingerprints, facial recognition and other biometrics can make banking more secure
By Amy McKeown, 3M

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

Early Alerts Spur Action (S18)
Why corporate security teams rely on social media for real-time information
By Dillon Twombly, Dataminr

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

Making Connections (F17)
The Internet of Things and the cloud bring new functionalities to the security industry – and new risks
By Mitchell Kane, Vanderbilt Industries

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

Smart Power (S18)
The paradigm has shifted to intelligent networking solutions
By John Olliver, LifeSafety Power Inc.

Diagnosing Security Challenges (F17)
Developing the secure hospital of the future starts with planning and collaboration today
By Marianne Iannotta, Kratos Public Safety & Security Solutions

Out of Many, One (S17)
Integrating components of a security system can vastly improve effectiveness
By Brian Wiser, Bosch Security Systems

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

24-Hour Perimeter Protection (S18)
Relentless defense for critical infrastructure
By John Distelzweig, FLIR Systems Inc.

A Laser Focus on Enhanced Security (F16)
New scanners can improve the accuracy and reliability of intrusion detection systems
By Patrick Hart, Optex

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

Navigating Technological Change (S18)
The way to success is ensuring new technologies impact your customers in a positive way
By Todd Graves, Allegion

Listen Up (S18)
How audio monitoring raises the surveillance bar
By James Marcella, Axis Communications Inc.

The Puppy Movement (S18)
A new vision for security
By Doug Haines, Haines Security Solutions

Securing Health Care Facilities (S18)
Maintaining 24/7 parking lot security
By Alex Doorduyn, Siklu Communication

Dialing Up Security (F17)
Smartphones can be an essential component of a mass notification system
By Jana Rankin, VuTeur

Getting on the Path (F17)
Shortest Path Bridging can enhance network performance and efficiency
By Darren Giacomini, BCDVideo

Augmented Reality is for More than Capturing Pokémon (F16)
When combined with IoT, the technology could have a big impact on security
By Rob Martens, Allegion

A Sound Solution in Transportation Security (F16)
Audio monitoring can enhance situational awareness, reduce crime
By Richard Brent, Louroe Electronics

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

Robotics/Artificial Intelligence

The Rise of the Machines (F17)
Robots can terminate tedious tasks for security personnel
By Alice DiSanto, Sharp Robotics Business Development

The Not So Friendly Skies (F17)
Drones represent a rapidly growing and evolving threat
By Nathan Ruff, Coalition of UAS Professionals

Combining Man and Machine (F17)
Robots can help human guards to be more effective
By Steve Reinharz,
Robotic Assistance Devices

Up in the Air (S17)
Drones powered by artificial intelligence could transform security
By Cary Savas, Nightingale Security

The Real Benefits of Artificial Intelligence (S17)
'Computer vision' powered by AI could radically change video surveillance
By David Monk, Umbo CV

Threat From Above (F16)
How can potentially dangerous drones be detected and defeated?
By Logan Harris, SpotterRF

Video Surveillance

Know a Lot About History, Know a Lot About Security (F17)
Data from cameras and other systems can increase understanding of events and contribute to a holistic approach to school security
By Jumbi Edulbehram, Oncam, and Steve Birkmeier, Arteco

VMS: The Next Generation (S17)
Facilities can now extend video management systems to provide a more complete security solution
By Shawn Mather, Qognify

Law & Order & Video (S17)
Police and prosecutors need enhanced case management systems
By Pota Kanavaros, Genetec

A Needle in a Video Haystack (F16)
Event-driven intelligence can identify the most important elements in surveillance data
By Steve Birkmeier, Arteco

Video Storage Wars (F16)
Hyper-convergence technology can simplify surveillance storage and enhance security
By Brandon Reich, Pivot3

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

Back to TOC

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 by emailing SIA at info@securityindustry.org.

securityindustry.org/techinsights

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