Look, Up in the Sky
What is the best defense against drone attacks?

Machine or Mannequin
Robots can ease the burden on human guards

Dial S for Security
Smartphones are a critical part of mass notification

SIA TECHNOLOGY Insights

Volume 5, Issue 2
Fall 2017

Welcome

Dear Reader,

Robot guards. Drone attacks. The Internet of Things.

The security industry continues to evolve rapidly. And for good reason – the threats that we are defending against are changing just as quickly. Technology has always had both good and bad applications, and this edition of *SIA Technology Insights* provides multiple examples of that.

Unmanned mobile devices have the potential to make security systems more effective and cost efficient, but they also represent a potential new threat vector that practitioners must be aware of. The Internet of Things enables the aggregation of massive amounts of data that can greatly enhance situational awareness, but it can also open up new vulnerabilities to attackers anywhere in the world.

The articles that follow offer valuable insights into how to maximize the ability of these and other technologies to enhance the protection of people and property, while mitigating the risk that arises from their misuse. Knowledge is an invaluable defensive tool.

Remember that all editions of *SIA Technology Insights* are available online at www.securityindustry.org/techinsights. We welcome your feedback about the articles, as well as your thoughts about this new age of security. You can contact the publication's editor, Ron Hawkins, at rhawkins@securityindustry.org.

Thank you for reading.

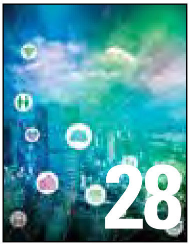
Sincerely,

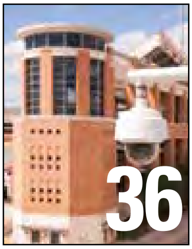
Denis Hébert
Chairman, Board of Directors
Security Industry Association

Don Erickson

Don Erickson
CEO
Security Industry Association

Table of Contents

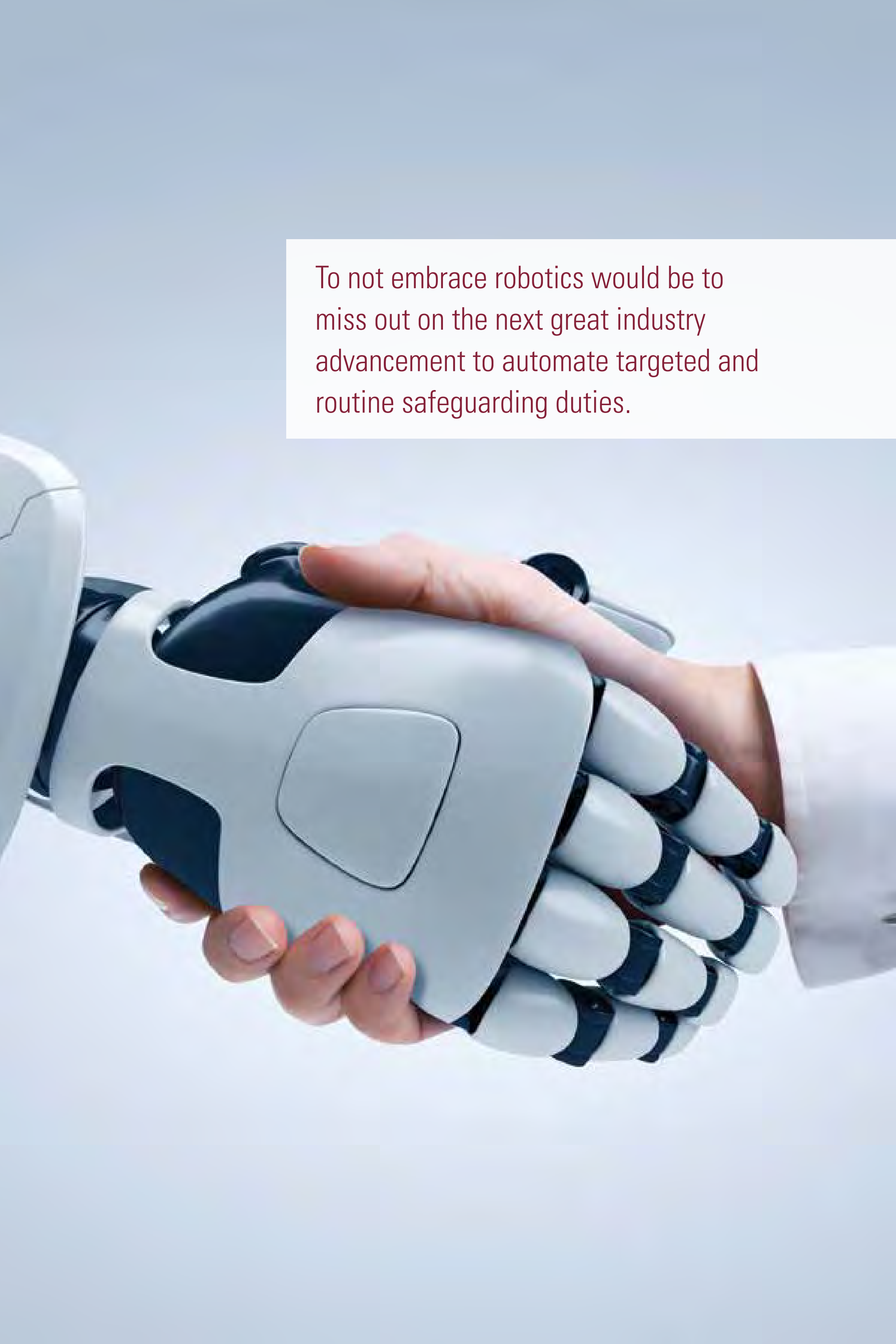



36

42

50

60



To not embrace robotics would be to miss out on the next great industry advancement to automate targeted and routine safeguarding duties.

The Rise of the Machines

Robots can terminate tedious tasks for security personnel

By Alice DiSanto
Sharp Robotics Business Development

Suppliers of air, land and sea robots appear to be in full agreement that these technologies will liberate people from routine guarding tasks, which are repetitive, mundane and at times dangerous, so they can shift their attention to more critical, intelligence-based work.

Who would not rally around handing off certain unfavorable parts of a job to a robot? After all, we have seen or experienced robotic successes in other applications, such as auto-attendant, airport check-in, manufacturing assembly lines, and the stocking of distribution center shelves. In these examples, robotic automation has led to greater speed, efficiency, quality and productivity. One need only think about the holiday shopping season and the exponential improvements that have resulted from online retailers implementing automation that speeds the fulfillment of orders.

The security industry is ripe to incorporate robotic technological advancements into the protection arsenal. Worldwide spending on robotics and related services in 2020 is projected to be double what it was in 2016. To not embrace robotics would be to miss out on the next great industry advancement to automate targeted and routine safeguarding duties.

That said, not all robot manufacturers are created equal. Optimism about the technology is best balanced by critical thinking throughout the evaluation process to find the right solution. Here are some key consideration points when identifying the right resource to satisfy a facility's security needs.

Understand Customary Capabilities

Robots can be deployed to defend against intrusions, respond to disasters, and inspect for vulnerabilities, while allowing their human counterparts to remain safely apart from frontline threats. They operate in either semi-autonomous or fully autonomous mode. Their capabilities, however, should not be exaggerated or overstated to the point of Hollywood fiction. Instead, the focus should be on what robots are customarily good at versus what humans do well.

Be an early adopter, but shop with discretion.

Robots are good at:

- Tireless operation
- Performing repetitive tasks consistently
- Operating in dangerous environments
- Recording events
- Real-time location and activity information

Humans are good at:

- Complex decision-making
- Multi-sense and unclear object perception

- Interacting with people; giving and understanding information
- Responding to random situations
- Undefined object or pattern identification

Collaboration and Automation

Together, man and machine can increase the effectiveness of security solutions and create better outcomes. The caveat is that you must select a robot that has been tested and approved for safe operation around people and objects in order for true collaboration to take place. Be sure to ask your provider for documentation (or a certification) of safety and reliability testing. Do not just assume that the tests have been run and third-party validation has been made.

> Their capabilities, however, should not be exaggerated or overstated to the point of Hollywood fiction.

Once you have found a product that has been safety tested, put it to work under the direction of your trained and experienced guard force. Allow your personnel to make process improvements using the new technology. Your human security force has a wealth of frontline know-how that can be used to delegate the full spectrum of required tasks, customize the technology to your exact needs, and enable you to cover operational shortfalls that, without robotics, were too time-consuming, too risky, or simply impossible.

Look Under the Hood

This is meant literally and figuratively. Given the ease of rudimentary construction, almost anyone can build a robot these days. Know the reputation and staying-power of the company that will be supplying the robot. What is the firm's track record of engineering, manufacturing, logistics, and maintenance? Is there a succession plan for the technology to remain state-of-the-art? Will the company be around to support the product through its entire lifecycle?

Next, actually look inside the robot. Is the design clean or is there a tangle of wires? Has the hardware undergone environmental extremes and endurance testing? What about the software? Is the interface intuitive and clear? Do the hardware and software truly work in tandem, with full operational control and telemetry?

Network Design is Key

Given the sensing and communication features of the security robots entering the marketplace, you need to have peace of mind that the data being procured and transmitted is kept confidential. Question vulnerabilities of disruption or interception. Is the network susceptible to hacking due to lack of encryption and dedicated IP addresses? What about the speed and bandwidth? The network is the direct line between the robot (or robots) and the brains of your security command center. The supplier should have a plan to address your need to maintain control of the technology traveling around the complex and to preserve the proprietary data that it collects.

Change Is Never Easy

Technological changes require adaptation, and that creates challenges. Who has not purchased the latest cell phone and experienced either user-error frustration or an operational glitch? When you do not understand the impact of a new technology, or it does not work exactly as expected, everyone around is in turmoil. This reaction to change happens every time a fresh technology emerges.

Think of the introduction of the automobile. Cars were a replacement for horse-drawn carriages, which congested urban streets with thousands of horses and the 35 pounds per day of waste produced by each horse. Though the automobile rid cities of a huge "dirty" problem, putting them into use brought about pains of change for communities. There were the usual user-errors and operational glitches, but the technology also had a broader impact because cars created a need for enhanced infrastructure, gas stations, traffic laws, etc. Similarly, introducing robotics into the workplace, for all the benefits that will result, will inevitably create issues that need to be addressed.

Robotics will bring about a change in job descriptions within organizations, and not just in the security department. Fresh opportunities will emerge with the adoption of automation. Certain functions will become outdated and companies will reduce the headcount for security tours and safety inspections. At the same time, though, they will add openings for robot operators and technicians.

Look for a supplier that acknowledges the fact that change, on both the individual and organizational levels, is hard.

Look for a supplier that acknowledges the fact that change, on both the individual and organizational levels, is hard. Pick a supplier who offers training, tools and techniques to ease the technological transition and accelerate adoption.

There Will Be Edsel Moments

Sticking with the automobile theme, some of the robots introduced to the security market will either be marketing failures, like the Ford Edsel, or will be criticized for some sort of shortcoming. As you evaluate your robot supplier, do not allow negative headlines to get in the way of the gains that can result from integrating robotics as a security solution.

Some suppliers will experience major Edsel-like failures because they did not thoroughly research their target market's needs. As for negative press, mistakes are inevitable. But from error should come improvement, so look at how the supplier recovers from the situation and notice if missteps are repeated.

The Time Is Now

Robots for security are an investment. The products you choose should integrate with your current infrastructure of people and technology. If upgrades in network are required, understand that this outlay will also support a wide variety of voice, video and data applications in other areas of your organization.

Optimism about robotics technology is well-founded. Overly positive assumptions can lead to problems, but the bigger picture is that you do not want to be left behind. Be an early adopter, but shop with discretion. A balance of enthusiasm and critical thinking when it comes to technology will keep expectations in check. To make progress, we need to imagine better solutions to our current challenges. Many of the risks we face are being perpetrated through malicious uses of technology. Having robots on our side to better protect people, infrastructure and assets strengthens the security industry. ■

Alice DiSanto (disantoa@sharpsec.com) is the director of marketing for Sharp Robotics Business Development (www.sharpintellos.com).

It is crucial that security professionals understand the potential threat vectors a drone could leverage and implement measures to deter such intrusions.

The Not So Friendly Skies

Drones represent a rapidly growing and evolving threat

By Nathan Ruff
Coalition of UAS Professionals

Unmanned aircraft systems (UAS), better known as drones, are making headlines frequently.

Drones drop grenades on Coalition Forces.

Drones land radioactive material on the roof of the Japanese prime minister's home.

Drones steal industrial trade secrets by hovering outside a 30th floor window while spoofing a printer's MAC address.

And the list is only getting longer and more troubling.

To be specific, the drones in the above instances are officially denominated as sUAS (small unmanned aircraft systems). These are not the large, military-grade MQ-1 Predators or MQ-9 Reapers carrying 800-pound munition payloads. Rather, this class of drone is defined as weighing less than 55 pounds "wet," which includes all peripherals. The classification includes rotorcraft, fixed wing and hybrid varietals, each with its own specific strengths and weaknesses. For example, if the goal is to deliver contraband to someone inside a prison's walls, a rotorcraft, given its ability to hover precisely, small noise signature, and capability to be operated from miles away, would likely be the preferred choice. If, however, speed, distance and the ability to carry heavier payloads were priorities, than a fixed wing drone would be a better alternative. The options are many, which makes defending against the threat more challenging.

To further complicate the situation, drones are popping up everywhere. The FAA estimates that 2.5 million drones were sold in the United States in 2016, and the agency projects that, by 2020, more than 7 million drones will be operating in the national airspace. Remote controlled aircraft have been around since World War I, but it has only been in the past 12-18 months that this rapid growth has occurred. Although component miniaturization, advances in batteries, and accelerated processing power were required for this technology to go mainstream, what has really driven the drone phenomenon is GPS stabilization. In the past, piloting a remote controlled aircraft took considerable skill and practice. That is no longer the case. Mastering the skills required to fly a drone over a prison wall, or position it 400 feet above the ground to snap photos of a secure facility, takes only about 15 minutes of practice. In fact, it usually takes longer to get the drone out of its packaging than it does to learn to fly it competently.

All of this has led to the proliferation of these advanced airborne robots at a price point at which they can be disposable items. Need a drone that is capable of spying on a neighbor or delivering a chemical agent? For around $400-$500, you are ready to start flying. And since drones are not

required by law to be registered or to have any identification markings, they can be abandoned with little concern after completing their nefarious missions.

Defenses and Regulations

So how great a risk do drones pose to the modern security professional? As usual, the answer depends on the specifics of the situation. For some, drones will merely represent a nuisance with no real operational implications. For others, the potential threat is much more significant. The former is best classified as a dumb actor scenario – someone flying a drone with no respect for privacy, nor a clear understanding of regulations, local ordinances, and safe operating protocols. This type of intrusion is best handled by enhanced awareness. A counter-UAS system will alert security of the incursion, triangulate the offender's location, and facilitate a response. Should that not work, local law enforcement can be called based on traditional statues such as trespass, reckless endangerment, and invasion of privacy.

On the other end of the spectrum is the bad actor scenario. This is when someone is using a UAS to gather confidential information or to create a threat to life or property. Because the UAS industry is nascent, regulations are lagging. Outside of

> In the past, piloting a remote controlled aircraft took considerable skill and practice. That is no longer the case.

the U.S. military, there is currently no legal way to actively neutralize a drone threat. UASs are technically unmanned aircraft, and it is illegal to shoot down, disable or interfere with the flight of any aircraft in the national airspace. Thus, physical interdiction is off the table. Furthermore, jamming, hacking, spoofing, or actively taking command of the drone by interrupting its radio frequency crosses a Federal Communications Commission (FCC) line and is also illegal.

The Federal Aviation Administration (FAA) controls the airspace, but it is not equipped to police the skies. Fines and revoked credentials are the limited tools they wield, and they do not have the manpower to identify most perpetrators. It is not a surprise, then, that the private sector has begun to fill the gap with myriad counter-UAS solutions. Ray guns (directed energy emitters), jammers, spoofers, predator drones, nets, and even trained birds of prey are just a few of the options making their way to the market. These technologies may be the future, but without the ability to deploy them legally, no security practitioner should consider such a purchase unless there is an operational agreement in place with a governmental agency. Outside the United States, there is a much more conducive environment for active countermeasures. All of this poses a major conundrum for anyone needing to defend against a bad actor scenario. Numerous interagency working groups and task forces have been formed to figure out a regulatory solution, but it will take time.

Regulations regarding both flights over people and micro-UASs have stalled because of concerns raised by the Department of Justice, the

Department of Homeland Security, the FBI, the intelligence community, and law enforcement about how to identify drones in the air. Their argument is that, without the ability to track UASs, understand who is operating them, and have in place a mechanism for accountability, drones should not be flying over people. The latest estimate for when a rule could be released for flights over people is May 2018.

There are many technological solutions to these challenges in the works, but, again, the process of testing, legalizing and implementing them is not fast. One good way to start sorting out "good actors" from "bad actors" today is to simply require UAS pilots to file a flight plan similar to how manned aviation has operated for more than a century. Submitting an unmanned operating area (UOA) notice takes about 30 seconds to accomplish, provides critical information regarding the altitude and timing of operations, and is a great way to improve the situational awareness of not only other UAS pilots, but the entire manned aviation community, as well. One app, for example, allows users to easily file UOAs from a phone or tablet, and the notification is instantly visible in the flight briefing system that 80,000 manned aircraft pilots use each week. Obviously, a "bad actor" would not use the system, but, by understanding who is playing by

Swarms of killer drones may seem like science fiction, but the technology required to make them a reality exists today.

the rules, identification of rogue flights becomes a much more transparent process. This, coupled with ADS-B or SIM card technology that has become small enough to be viable on drones would allow everyone operating in the national airspace to both "see" and "understand" the intentions of drones in flight.

Threat Vectors

Until the day comes when all drone flights are conspicuous, it is crucial that security professionals understand the potential threat vectors a drone could leverage and implement measures to deter such intrusions. Understanding how UASs can be used maliciously will enable security practitioners to think through this new class of vulnerability and facilitate creation of a strategic defense. Delivery threats (both physical perils and contraband delivery) and intelligence gathering represent two main areas of susceptibility for the security industry.

In terms of delivery threats, the ability to put a 9mm firearm on a drone and operate it remotely with a disturbing degree of accuracy was proven by an 18-year-old in Clinton, Conn., in 2015 in a viral video. The exhibition, though, also highlighted an important limitation, in that firing a percussive weapon from a UAS platform creates substantial kickback, resulting in temporary destabilization. Although multiple shots were fired, this was effectively a "one-and-done" threat with regard to most real-world situations. However, a recoil suppression gimbal is now available that allows a sniper rifle to be mounted on a UAS platform and fired multiple times with a high degree of accuracy.

Because it is common practice for agricultural drones to spray crops, the potential to use a drone to disperse dangerous biologic agents is obviously a concern. The ability to fly a drone into a population center and drop microorganisms from above depends only on access to the bioweapon; the delivery vehicle is readily available and its purchase is unregulated. ISIS uses drones to drop modified grenades, but this is a rudimentary first step. Microscale reactive ordnance as a payload represents a more significant threat given its "weight-to-bang" ratio. Thinking a little bit more creatively, mounting a thermal breeching tool on a drone platform presents additional threats. The flashlight-sized device can cut through a half-inch steel bar in less than a second while burning at 5,000 degrees Fahrenheit.

Capturing meaningful data from above is no longer a complicated operation; it is big business.

"Swarming" represents a particularly unsettling delivery threat. The potential for UASs to be leveraged as asymmetrical warfare tools has already been discussed, but extending that concept to a swarm of drones operating with a common objective and controlled by a single pilot poses exponentially greater risk. One drone can do damage, but imagine 500 drones operating in concert: a minefield in the sky that cannot be skirted or easily neutralized. Combining this concept with autonomous operations and some degree of artificial intelligence, one can start to imagine a formidable future threat. A drone swarm could comprise "bombers" and "specialists," similar to the division of labor found in an ant colony. Specialist drones could be tasked with mapping any new environment the swarm enters with simultaneous localization and mapping (SLAM) technology, assessing/overcoming threats, capturing intel, etc., while the majority of the swarm is equipped to drop ordnance or simply launch kamikaze attacks into designated targets. At this point in time, UASs flying in cooperation can create networks, transfer information, make deliveries, or even "dance" (as demonstrated during the 2017 Super Bowl halftime show). Swarms of killer drones may seem like science fiction, but the technology required to make them a reality exists today.

Gathering intelligence is the second main area where UASs have proven to be a disruptive technology. PwC estimates that drones represent a $127 billion global market, and the Association for Unmanned Vehicle Systems International (AUVSI) projects the creation of 70,000 new jobs in the sector in the United States over the next three years alone. One of the reasons behind this growth is that collecting information from above historically required a helicopter, fixed wing airplane or satellite, so the savings that UAS technology provides are huge. To complement these new aerial platforms, sophisticated sensor packages are available off the shelf that provide thermal imaging, 6K video, or 50-megapixel stills. In addition, magnetometers, facial recognition and airborne chemical analysis are other areas where drones could potentially perform better than current solutions. Capturing meaningful data from above is no longer a complicated operation; it is big business. So what does the near-term future hold for this rapidly evolving technology? The likely answer is automation and integration.

Automation and Integration

Fully autonomous flight is the future: UASs capable of flying missions without a person at the controls. This already exists to some extent, and advances in machine vision and machine learning (artificial intelligence) have been truly impressive. Not only can drones "see" obstacles in their path, they have the onboard processing power to make adjustments so that the sortie can be completed. Soon, humans will set the objectives, and airborne unmanned robots will execute the mission.

UAS integration into the Internet of Things is happening now. Taking the concept of automation to the next level, consider the type of information that will become available if every drone flight is not only performing its intended assignment, but is also simultaneously capturing and sharing information about its environment. This can include, say, real-time pictures of traffic conditions, weather, or crop growth. Or, more troublingly, what time your car is parked in front of your home, when you go for a jog, or who visits your house. The U.S. Army recently banned drones from a Chinese manufacturer because of the potential to covertly record and transmit information back to that country.

Autonomous vehicles and autonomous drones are traveling on a parallel path. In fact, since the technology is analogous, a number of manufacturers are investing in both markets. The idea is that autonomous vehicles will need to have an up-to-the-millisecond picture of roadways in order to operate safely. Thus, if a box falls off a truck on the highway, the first vehicle behind it feeds that new information into the global database so that all other vehicles headed in that direction are aware of the potential hazard. Drones represent one more node of data collection to feed into this master picture.

> Soon, humans will set the objectives, and airborne unmanned robots will execute the mission.

It is clear that drones are a new and rapidly developing threat vector. The technology also represents a sea change for security services desiring to integrate drones into their portfolio of solutions. The ways that drones can be used to compromise security seem limited only by the imagination, so the ability to counter these new threats will require thinking beyond traditional approaches. Devoting the time and effort to assess how exposed assets are to this type of peril and, if necessary, crafting an interdiction strategy is an exercise well worth undertaking. ■

Nathan Ruff (nathanruff1@gmail.com) is the executive director of the Coalition of UAS Professionals (www.uascoalition.org). He also manages NKR Partners Consulting Group (www.nkrpartners.com).

Within the security market, robots are emerging as a way for businesses to augment existing security patrols and provide greater situational awareness.

Combining Man and Machine

Robots can help human guards to be more effective

By Steve Reinharz
Robotic Assistance Devices

It may seem like science fiction to envision a world in which robotic devices are commonplace, but it is more realistic than one might think. Robots that leverage artificial intelligence (AI) are already in use in a wide variety of markets and applications. In manufacturing, robots are used to increase productivity and streamline the production process. They are also used to reduce the need for human personnel in mundane and repetitive roles. This allows companies to shift people to more valuable and higher-paying positions, such as those found in customer service, marketing, operations, and management, to increase morale and enhance operations.

For example, Seattle-Tacoma International Airport recently began testing a new use case for robots that provide tips to travelers on getting through security more quickly. The robot, stationed near screening areas, directs passengers to remove their jackets, take off their shoes, remove laptops from bags, etc. This tedious job that TSA agents would otherwise be performing can now be outsourced to a robot, freeing up airport employees to address more complex matters that can enhance security and efficiency.

Using Robotics in Security

The Sea-Tac example is just one of many that demonstrates how today's advanced robotic solutions are being used. Within the security market, robots are emerging as a way for businesses to augment existing security patrols and provide greater situational awareness. And we have only begun to scratch the surface of what robotics can do to improve day-to-day operations.

Security robots can bring substantial benefits to businesses. They can patrol the perimeter of corporate campuses or critical infrastructure sites to identify potential trouble spots; remove traditional guards from dangerous situations; detect individuals or vehicles in unauthorized areas; and integrate with existing sensors and systems to allow operators to gain new levels of intelligence and insight into situations.

How does it work? Information gathered through sensors on the robot, such as video surveillance cameras, navigation equipment, motion detection, microphones and facial recognition software, is transmitted to a security operations center. The information is then analyzed and combined to create a complete picture of a situation that security personnel can use to make an informed decision on the most appropriate course of action.

Where Robots Are Used

Security robots can meet needs in many markets, but they are most valuable in large facilities, such as utility companies, oil and gas production sites, and education and corporate campuses. Robots deployed at these kinds of locales can patrol dangerous or hard-to-reach spots and provide surveillance of large areas more efficiently than human guards.

In these cases, robots serve as an extension of existing security operations and a manned guarding contingent. Expansive areas where numerous guards would need to be present to offer full coverage can be served well by robots that offer additional "feet on the ground."

Robotics and AI

As mentioned above, security robots use multiple sensors and bring the information together. Open-platform applications work together seamlessly to collect and analyze data. AI software is embedded to provide security officials with the ability to analyze the images captured by on-board cameras. The information gathered through this and other sensors on the robot is critical to the implementation of a comprehensive strategy and tactical response.

Advanced object recognition is what enables a robot to become a core part of the enterprise security team.

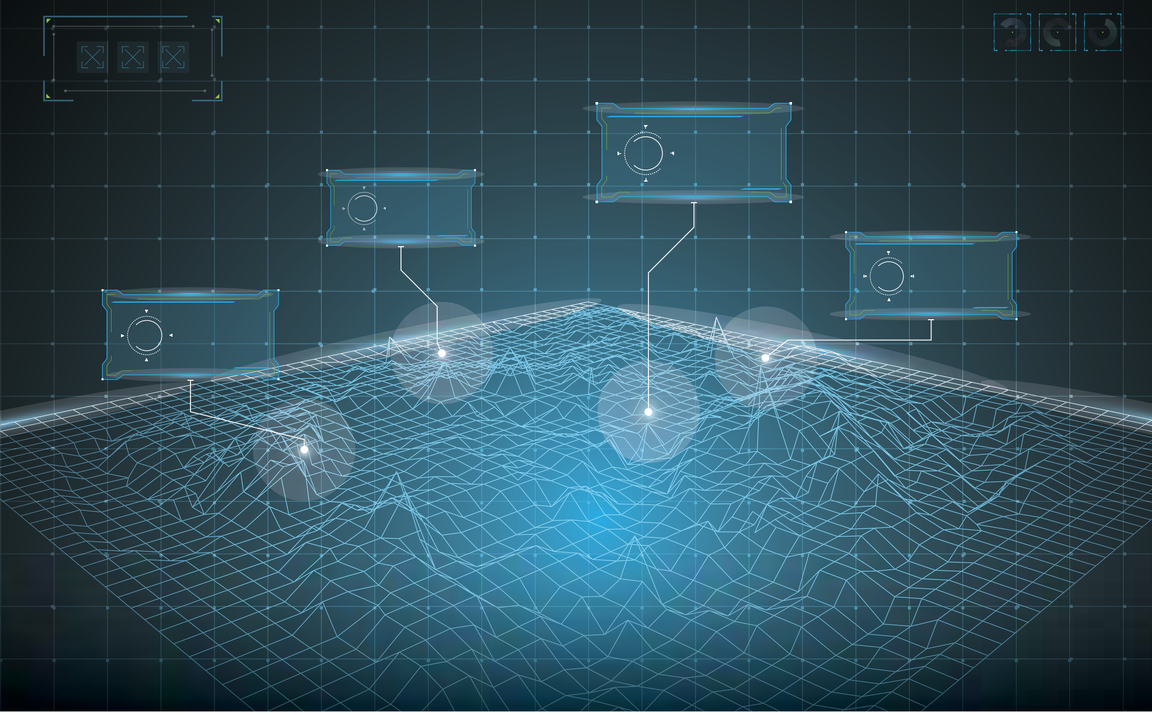
Additionally, through the use of advanced AI technologies, robots can "learn" their surroundings. They are initially programmed to navigate a particular route, but as they continue on this path numerous times, the robot can make adjustments. AI makes this possible by giving the robot the "brains" to engage with its surroundings. This approach has the potential to add significant value to patrols.

AI also makes it possible to recognize patterns within large amounts of collected data. In the case of robotics, this can include automatically searching through video surveillance feeds for anomalies. Security-based AI, however, is narrower in focus, executing certain defined tasks such as object recognition or navigation. Advanced object recognition is what enables a robot to become a core part of the enterprise security team. Leveraging this type of AI allows robots to identify when a human or vehicle is approaching a perimeter and then execute a set of procedures in line with an organization's goals.

> The partnership between human and robotic guards creates numerous advantages, including advanced patrolling capabilities and added responsiveness.

Guards and Robots: A Natural Fit

Innovations in robotics and AI have some security professionals fearful that robots will one day "take over" human responsibilities. That



is not the case. In fact, robots and people work best when they work together. With the robot revolution upon us, guarding companies see the value of these solutions and aim to take advantage of their capabilities. There are more than 1 million security guards employed in the United States, according to the U.S. Department of Labor's Bureau of Labor Statistics, and that number is growing. The partnership between human and robotic guards creates numerous advantages, including advanced patrolling capabilities and added responsiveness.

Robotics providers are finding ways to seamlessly integrate their technology with guarding companies by offering additional ways to collect information and send it back to an organization's security operations center. Some of the largest guarding companies in the United States recognize the value of robotics in decreasing the number of "dangerous" roles assigned to people, reducing liability and potential accidents. For example, it would be costly, and perhaps unreasonable, to post a person at a utility site that is hundreds of miles away from a corporate facility.

Some of the largest guarding companies in the United States recognize the value of robotics in decreasing the number of "dangerous" roles assigned to people, reducing liability and potential accidents.

However, a robotic guard would be a perfect fit. There are also some toxic waste dumps where protection is needed, but a human presence is best avoided.

Robots can also be useful in more mundane jobs, such as working a late-night shift performing perimeter checks several times each hour. Redistributing such monotonous work frees human security guards to take on more strategic tasks, and saves employers health care, labor and insurance costs.

Best Practices for Implementation

For many enterprise organizations, security robots are an emerging concept and a new addition to a comprehensive security strategy. Therefore, certain considerations must be taken into account before the implementation of the technology – especially when human guarding is used, as well. Here are some tips for implementing security robots into an organization:

- **Know the technology uses** – Before any robots deploy, an organization must decide what it wants to get out of the investment. Will robots be used strictly for perimeter security? Just for remote locations? Only during large-scale events? These decisions should be made before any change in strategy is implemented.
- **Educate the team –** Robotics, in general, can have a negative connotation, leading human guards and other security team members to wonder, "Am I being replaced?" The best way to handle this concern is to maintain constant

communication about the changes being made. This can be accomplished through seminars, announcements in team meetings, or training sessions that outline exactly how the robots will be used and why.

- **Provide training –** Security robot manufacturers are in the business of ensuring that their technology is used as efficiently and effectively as possible, which means training is crucial to the deployment process. Identify anyone who will be working with the robots and give them the opportunity to take courses on how best to use the technology.
- **Develop standard operating procedures for robot use –** Introducing robotics makes it mission-critical to provide new SOPs. If a security operations center is in use, these procedures must also be put into the database so that security guards who are monitoring the robot's patrol can go through the proper steps in the event of an incident.

Robotics can provide significant value in various applications. It is critical for enterprise organizations to weigh the costs and benefits of implementing this new and innovative technology to meet today's and tomorrow's business needs. As security robots continue to produce strong improvements to customers' programs, they will become as ubiquitous as their human guarding partners. ■

Steve Reinharz (steve.reinharz@roboticassistancedevices.com) is president of Robotic Assistance Devices (www.roboticassistancedevices.com).

A benefit of using connected devices for access control is forming a complete picture of an organization’s ingress and egress points, which can increase insight into throughput rates and traffic patterns and provide the ability to look at an individual’s usage.

Making Connections

The Internet of Things and the cloud bring new functionalities to the security industry – and new risks

By Mitchell Kane
Vanderbilt Industries

Connectivity worldwide is thriving. A report by Gartner forecasts that 8.4 billion connected devices will be in use worldwide in 2017, up 31 percent from 2016, and that number will reach 20.4 billion by 2020. Everything from a house's microwave and heating/cooling system to cars and TVs are connected, leaving many to wonder: What's next? Connectivity is a hot topic in the IT world, especially, as more and more devices communicate with each other to streamline operations.

For those in the security industry, the next frontier seems to be incorporating several ideas from the realm of connectivity: the Internet of Things (IoT), the cloud, and web-based interfaces that allow flexibility for users. But how can the industry integrate these tools into the day-to-day security operations of an organization? This article explores the challenges that users face, how those challenges can be overcome, and how the industry is coping with the emergence of these technologies.

The Internet of Things

The IoT introduces a new capacity for connectivity that is proving to be a real benefit for enterprises. At its basic level, the IoT is the concept of connecting any device with an "on/off" switch to the Internet and, in some cases, to other devices. So how does the IoT work in the realm of access control technology? Advanced connectivity through smartphones and other devices allows for a much more personalized experience by using mobile credentials, biometrics and analytics in new and innovative ways. Smartphones and wearable technologies, such as wristbands, can be used for mobile credentials and allow access to certain sections or rooms within a building. More specifically, readers can recognize these types of devices to grant access when authorized.

When a company is building or updating its security solution, attention to cyber threats is crucial. Therefore, it is critical that the IT department is pulled in to ensure proper data safety protocols are being followed.

A benefit of using connected devices for access control is forming a complete picture of an organization's ingress and egress points, which can increase insight into throughput rates

and traffic patterns and provide the ability to look at an individual's usage. Additionally, this level of connectivity through network-enabled devices allows enterprise organizations to set "rules" that can be applied depending on the time of day or day of the week, or occurrence of special events, making the possibilities of streamlined access nearly limitless.

One challenge that the IoT presents for enterprise organizations is how access control can best be implemented to encourage security and privacy. Systems integrators, dealers and security consultants play a crucial role in the deployment of access control systems that use advanced IoT-enabled devices, but businesses bear the burden of understanding and communicating best practices to end users to protect organizations from risk. How does an enterprise manage this endeavor? By adopting a user-centric design with scalability, tactical data storage and access with appropriate identification and security features. The connectivity that the IoT represents means that leaders must stay one step ahead of threats to curb their negative impact on an organization's goals.

> Cloud-based access control and video management has emerged as a solution that benefits small to medium-sized businesses that do not have the capital needed to engage advanced security solutions in-house.

The Cloud and Web-Based Solutions

The cloud is a mystery to many, but it is growing in popularity, leading many companies to seriously look at ways they can utilize the tool in their own businesses. Capital investments in hardware that stores data in-house can be costly, limiting an organization's ability to upgrade to newer, more advanced functionality as it becomes available. One advantage that the cloud offers to these businesses is cost-effective management of data. For example, in the past, people would run applications or programs from software downloaded on a physical computer or server that was located in their building. Now, the same kinds of applications can be run through the Internet.

Manufacturers in the security market have found ways to harness the power of the cloud to benefit end users. Cloud technology has made it possible to remotely monitor multiple locations from anywhere in the world, as long as there is an Internet connection. More specifically, cloud-based access control and video management has emerged as a solution that benefits small to medium-sized businesses (SMBs) that do not have the capital needed to engage advanced security solutions in-house. Instead, they rely on web-based functionality to allow security directors to manage access points, be alerted to problems and monitor ongoing incidents in an easy-to-use manner. For this kind of solution, all that is required is a browser and an Internet connection.

> The acceptance of the cloud will grow as more businesses experience the benefits of it.

In late 2014, IHS reported that the global market size for access control as a service (ACaaS), such as cloud-based access control hosted and managed solutions, would top $530 million by 2018 and $1.8 billion by 2025. This means the business strategy for manufacturers providing cloud-based services is only expected to grow in the coming years, capitalizing on the demand from end users in this burgeoning market. This is especially true in the SMB market, where many would like to adopt more comprehensive security solutions into their operations but lack the resources. ACaaS offers these entities the ability to get upgrades without having to worry about servers and IT connectivity and compatibility.

Remote monitoring through smart device applications allows organizations to eliminate the need for in-person troubleshooting. Technical queries or issues can be diagnosed

and resolved on the go, delivering ultimate control to site security, which allows issues to be dealt with efficiently, minimizing disruption. For these businesses, all of this can be done without having to worry about managing the infrastructure associated with providing this level of capability.

Using a web-based platform allows oversight 24 hours a day, 7 days a week. If an alarm is triggered when a security manager is at another location or has already left for the day, or if the location is difficult to access, the manager can simply take out his or her smartphone or other Internet-connected device to view the event on an app, manage the response and turn off the alarm. Remote and web-based monitoring – and the ability to offer this kind of solution in a connected world – boils down to providing ease of use and convenience to end users. Remote monitoring through cloud-based solutions saves businesses time and money, while bringing peace of mind to security leaders.

One challenge the cloud faces is acceptance in the marketplace. Many end users have concerns about the security of cloud-based applications. However, the acceptance of the cloud will grow as more businesses experience the benefits of it. Very large enterprise-type users, though, may still feel more comfortable with their access control/security management system residing on the corporate

network, as a result of their investment and confidence in the security of that network.

The Importance of Collaboration

With this interconnectivity comes an increased risk of security threats. One of the greatest fears related to deploying cloud-based and IP-centric solutions is their vulnerability to outsiders wishing to do harm to an organization. As a result, cybersecurity efforts can no longer be ignored as organizations continue to integrate physical security products. The possibility and severity of a data breach rises significantly as more devices are added to a network. But, as many leaders know, increased risk does not automatically mean an increase in an organization's security budget or preparedness plans.

One solution to countering this hazard involves repurposing resources and experts that are already available: the IT department. IT professionals are already well versed in the ins and outs of a company's computers, network and software, and they share the goal of protecting critical data and keeping outsiders out.

When a company is building or updating its security solution, attention to cyber threats is crucial. Therefore, it is critical that the IT department is pulled in to ensure proper data safety protocols are being followed. A hack into an organization's private information can be catastrophic, and oftentimes intruders are looking for sensitive material relating to people's personal lives, such as Social Security numbers. Employing the help of an IT team can ensure that such data is comprehensively secured.

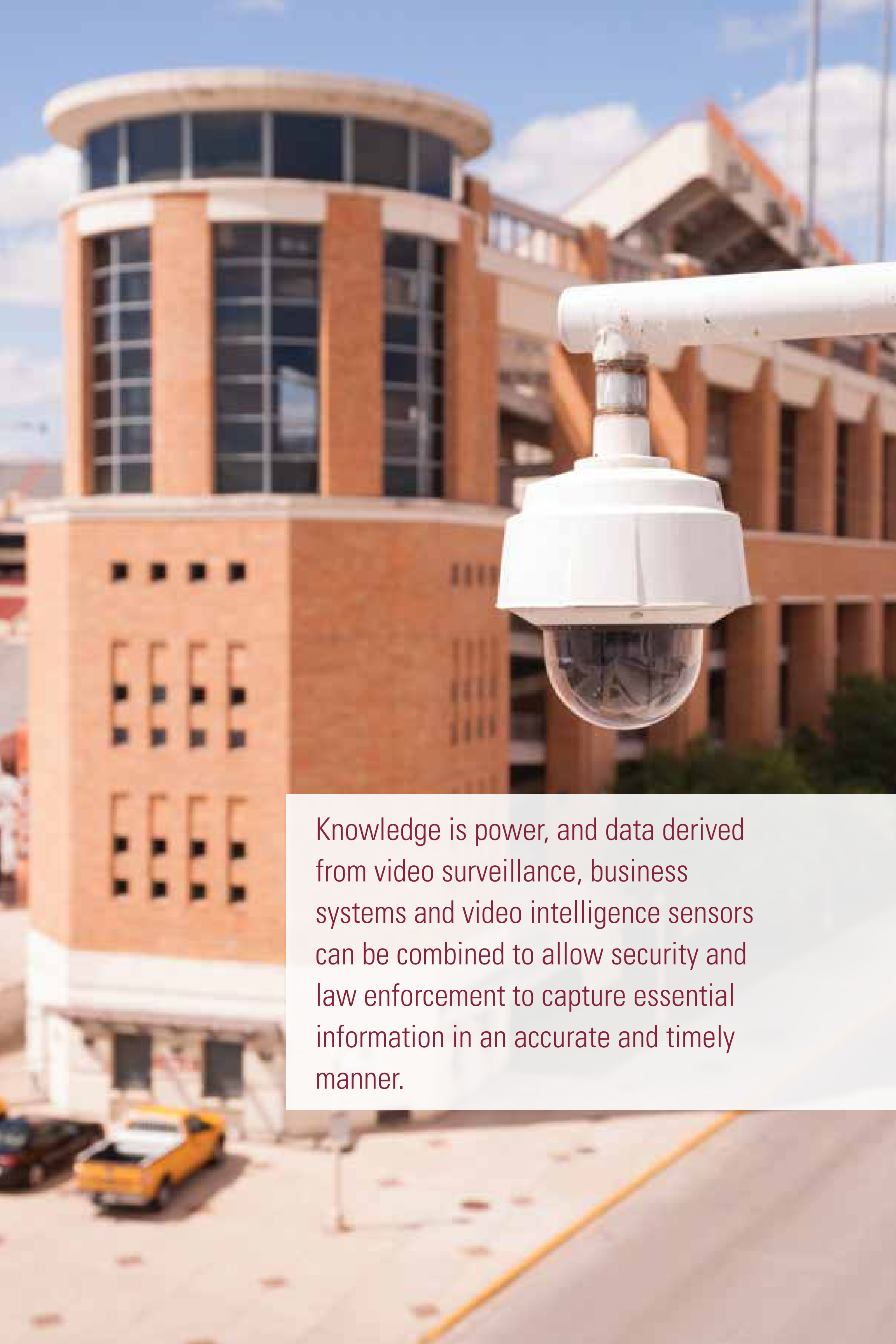
Additionally, IT departments can assist organizations in keeping up with new technology, such as software updates and patches, so that networks are not left vulnerable to outside threats. Technology and software are advancing every day, which leads to an expansion in the variety and intensity of cyber attacks. It is imperative to utilize a more advanced, exhaustive security plan that helps realize increased situational awareness and business intelligence.

The integration of multiple aspects of a security network into a unified system is very valuable, but it also creates more points of vulnerability. Encrypting communications between devices is therefore paramount. A single insecure structure or poor deployment can make the entire system vulnerable. IT and security teams must work together to protect each facet of a connected network to guarantee that the overall system is secure. The convenience of remote and instant access to security solutions must be weighed against the ability to keep data safe and secure from threats, and the expertise of an IT team can only strengthen the universal security of a business or enterprise organization.

Manufacturers can address the potential risks that the IoT and cloud-based solutions present by continually testing products for security vulnerabilities in order to provide a high level of confidence that the solutions are safe. Doing so bolsters consumer confidence and minimizes risk.

With technology continuing to embed itself into everyday life, it is important for the security industry to prove its agility, adaptability and dependability in keeping up with consumer needs. Remote and instant – and secure – access to solutions helps to do just that. ■

Mitchell Kane (mitchellkane@vanderbiltindustries.com) is president of Vanderbilt Industries (www.vanderbiltindustries.com).



Knowledge is power, and data derived from video surveillance, business systems and video intelligence sensors can be combined to allow security and law enforcement to capture essential information in an accurate and timely manner.

Know a Lot About History, Know a Lot About Security

Data from cameras and other systems can increase understanding of events and contribute to a holistic approach to school security

By Jumbi Edulbehram, Oncam
Steve Birkmeier, Arteco

Safeguarding campuses is a complex, multi-faceted process. The stringent requirements and security challenges of higher education and K-12 facilities propel users to seek out advanced insights to facilitate quick responses and more informed decision-making.

It is no secret that the occurrence of violence in schools is a very real threat. With the extensive media coverage of incidents in K-12 schools, as well as on college campuses, these facilities may no longer feel like safe havens for education. As a result, schools have adopted policies and security measures to combat modern-day threats in an effort to reduce the risk of violence. One such solution is the installation of video surveillance, security software and other technologies that can be integrated to create a comprehensive safety and security plan. From a process standpoint, school stakeholders strive to enhance security training, develop response plans and collaborate with other school districts to stay ahead of the game.

It is an unfortunate fact that real-world threats continue to multiply and expand within the education environment. According to the Centers for Disease Control and Prevention (CDC), 1 to 2 percent of all homicides among school-age children happen on school grounds, on the way to and from school, or during a school-sponsored event, and approximately

17.9 percent of high school students in 2013 reported taking a weapon to school. That same year, 19.6 percent of high school students reported being bullied on school property.

These statistics show that campus security teams must keep pace with changing trends and threats. In today's risk environment, schools can no longer afford to take a passive approach to security. Furthermore, the trend toward newer facilities and larger, expanding campuses necessitates more advanced systems, policies and programs – a holistic approach, if you will – to ensure protection for students, faculty and staff members.

The security industry focuses on developing technologies and services that enable higher levels of safety, increased intelligence and more proactive processes. Video surveillance solutions have proved valuable to schools of all types and sizes because these platforms help users identify notable events and potential anomalies, while allowing users to gain access to the most relevant video and security information at any given time. The focus is on identifying critical events and areas of interest, enabling stakeholders to use truly *intelligent* data (rather than non-critical video) to help ensure the protection of students, staff, data and infrastructure. The industry collectively tries to help schools access the most important information to produce more informed responses, increase

In today's risk environment, schools can no longer afford to take a passive approach to security.

situational awareness and improve overall security management.

Campus Security Trends

With the risk landscape expanding and the installed base of IP cameras growing significantly, campus security personnel need more ways to acquire intelligence from their technology investments. Moving forward, video surveillance systems are going to be judged based on how quickly and easily they can aggregate video within the new "big data" landscape.

Another trend that will have an enormous impact on video management systems is the proliferation of advanced video analytics, not just for security applications but also for operational efficiency. Schools will begin to find new use cases for video surveillance in the very near future. Here are some of the trends that will drive new levels of intelligence in campus environments.

Correlated Data

The best way to get a clear grasp on trends, events and incidents is to capture the whole story. Knowledge is power, and data derived from video surveillance, business systems and video intelligence sensors can be combined to allow security and law enforcement to capture essential information in an accurate and timely manner. Additionally, departments within schools, such as IT, security and operations, will continue to converge to streamline operations and develop more robust strategies that benefit the overall organization.

Intelligence

Having all of the information is the first step, but using it to create actionable intelligence is key. Combining video data with analytics gives officials the ability to better evaluate traffic flow and people's behavior patterns. Data analytics, meanwhile, examine raw data from various sources for the purpose of drawing usable conclusions about that information. These analytics can be used to measure student engagement and offer administrators an inside look at how students perform in the classroom, engage with lesson plans and understand the material.

Proactive Investigations

The ability to capture and store data, and transfer it cohesively across platforms, aids in the research and

Campus Security Coalition

The Campus Security Coalition was created to address the security concerns of educational institutions and help them maximize intelligence and security efforts. It is designed to bring together school leaders and other stakeholders and promote discussions about how to better address threats, strengthen security efforts and realize more effective intelligence efforts.

The coalition comprises educational end users, administrators, consultants, architects and technology providers. Members can use the valuable resources and information they acquire as part of the group to enhance school security plans.

Membership is open to professionals with experience in school security and safety initiatives, schools and school districts, educational administrators, consultants, campus police and security leaders. There are also opportunities for security product and service providers to participate. The coalition produces a newsletter that includes news and trends on security and safety, features on leading practitioners, and strategies and techniques aimed at helping position school security programs for success.

Grant Program

Faced with growing threats of violence, vandalism and other criminal activity, school systems are challenged with protecting people, infrastructure and assets while maintaining an open environment. Budget constraints often limit the availability of dollars for security enhancements. The coalition has developed a grant program that seeks to assist schools by partnering with leading technology vendors and installers to provide the tools and services necessary to strengthen situational awareness and security intelligence.

As part of this year's program, the coalition invites schools of all sizes and types to apply for a grant. One school will be selected to receive the hardware, software and additional equipment necessary to implement a security technology upgrade. The grant application period will close on Oct. 15, 2017.

The Value of Collaboration

Educational institutions have experienced a significant increase in threats that put the lives of students and faculty members at risk. While the demand for better security measures has risen, the adoption of new solutions can be hindered by a lack of cohesion across varying segments. By bringing stakeholders together, the Campus Security Coalition is seeking to enable more coordinated and effective approaches to school security.

analysis phase of addressing incidents. And the faster the data can be collected to be used forensically, the better the chances of solving a case. Being able to look back – and forward, in some cases – helps to resolve issues, as well as prepare for future threats. Schools need to adopt programs and solutions that produce the intelligence needed to be more proactive in overall security efforts.

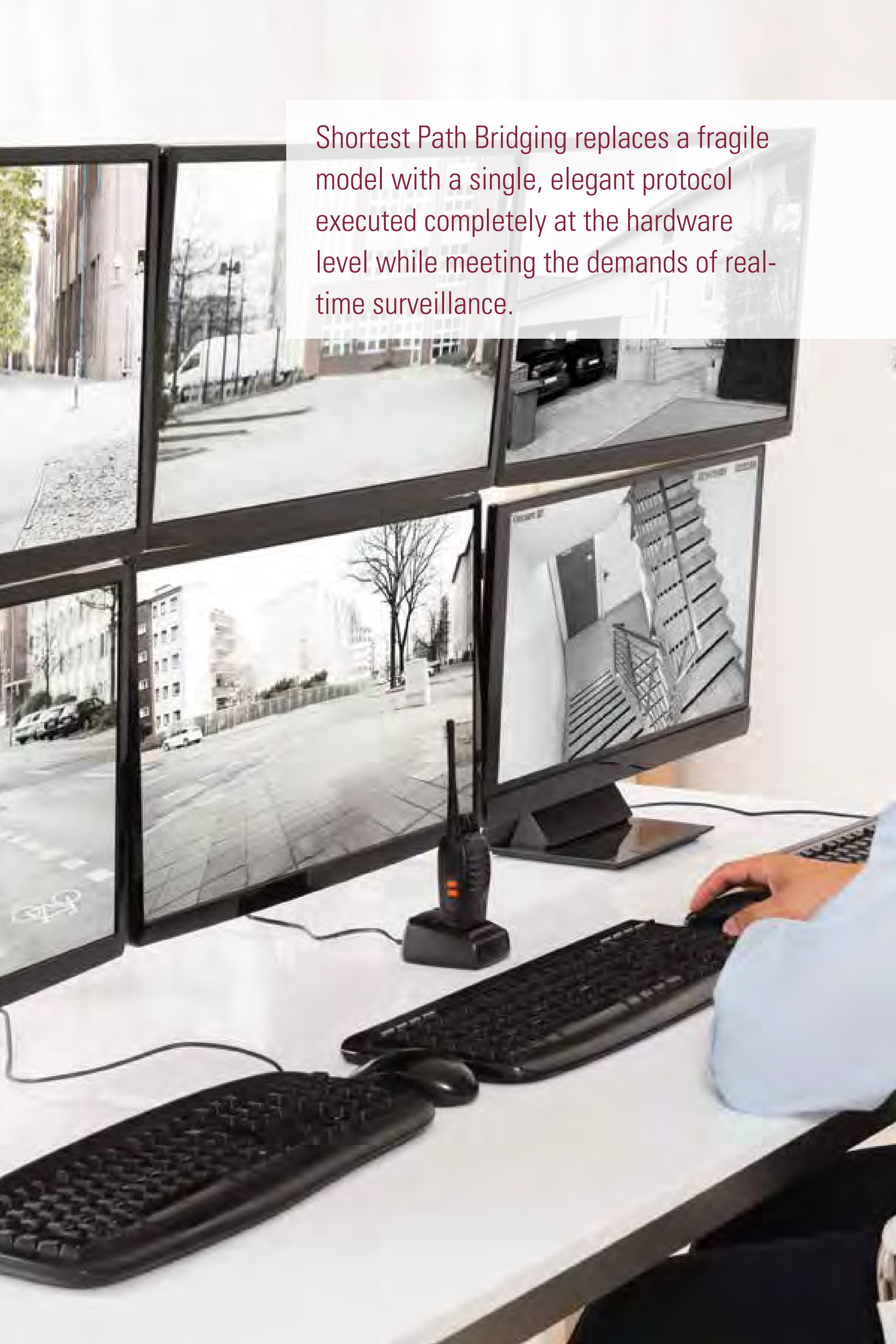
The focus is on identifying critical events and areas of interest, allowing stakeholders to use truly *intelligent* data to help ensure the protection of students, staff, data and infrastructure.

Open-Door Policy

Technologies that focus on easing the path to integration enable schools to correlate data points from multiple devices and systems. This approach allows stakeholders to combine information in one interface to create a full view of a situation at any given time. Combining video with other security and non-security solutions, such as fire and intrusion alarms, access control, emergency management equipment, IT systems, and building management, makes this possible.

The evolution of crime and threats has been met by the evolution of technologies to combat them. Using approaches such as those described above can enhance both school security and the learning environment. ■

Jumbi Edulbehram (jedulbehram@oncamgrandeye.com) is regional president, Americas, for Oncam (www.oncamgrandeye.com), and Steve Birkmeier (sbirkmeier@artecous.com) is vice president of sales and business development for Arteco (www.arteco-global.com). More information about the Campus Security Coalition is available at www.campussecuritycoalition.com.



Shortest Path Bridging replaces a fragile model with a single, elegant protocol executed completely at the hardware level while meeting the demands of real-time surveillance.

Getting on the Path

Shortest Path Bridging can enhance network performance and efficiency

By Darren Giacomini
BCDVideo

As the world of surveillance evolves, the introduction of multi-sensor and megapixel cameras presents a dynamic shift in industry accepted standards. For years, we have known the limitations of pan-tilt-zoom (PTZ) cameras, often finding them looking in one direction, only to miss critical events in another. To overcome this limitation, cameras were added to increase coverage.

While innovations in camera technology have addressed the shortcomings in PTZ models, network infrastructure has been placed under unprecedented levels of stress. As the capabilities of cameras increase, along with their coverage areas, so does the critical nature of their operation. In other words, if a single camera is covering one side of a stadium or an entire parking lot, the user cannot afford for it to go offline.

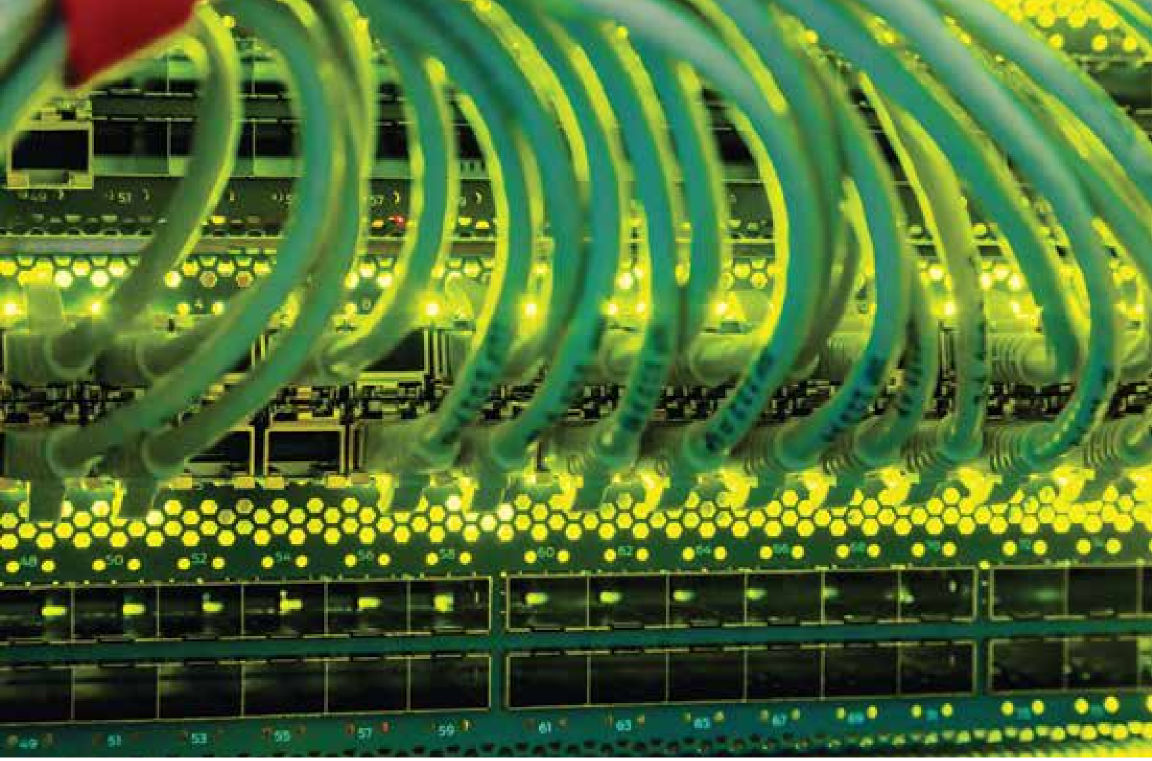
As the days of using proprietary networking hardware come to an end, networking vendors no longer develop their own application-specific integrated circuits (ASICs). Instead, they rely on "merchant silicon" for their networking product offerings. This allows all vendors to use the same hardware, while differentiation is based on the software features of the switch.

For decision-makers, just identifying the shift toward multi-sensor and megapixel cameras is not enough. More than ever, surveillance networks are depended upon to deliver high availability, resulting in "always on" video. Without the proper backend technology, though, an entire video system could go offline.

Without the proper backend technology, an entire video system could go offline.

Networking House of Cards

Shortest Path Bridging (IEEE 802.1aq) is based on the concept of simplicity – using a single protocol to perform the function of many and executing these functions at the hardware level. Traditional networking creates a house of cards, with multiple overlay protocols used to deliver the required network functionality. Protocols like RSTP, OSPF, IGMP, PIM and MSDP deliver functionality but only serve to prop each other up. Each one becomes dependent on its underlying protocol for operation. When those underlying protocols break, all dependent protocols cease to function properly. In other words, the house of cards comes tumbling down, and the user is left waiting for the rebuild. During this downtime, critical surveillance operations come to a grinding halt, resulting in video and archiving loss.



Shortest Path Bridging replaces this fragile model with a single, elegant protocol executed completely at the hardware level while meeting the demands of real-time surveillance.

Resiliency: You Get What You Pay For

A core switch will power down or need an update, or a primary network path will fail. It is inevitable. The effect this has on surveillance operations depends on the network topology and the technology it supports.

With traditional network technologies, convergence to the redundant path comes at a cost – video frames are dropped while the new path is established. While the network itself can recover in tens of seconds, it often takes the video management system (VMS) much longer. During this time, the user will not be able to record or access any live video.

> While most software-defined networking is in the data center, this emerging technology is starting to shape the way the surveillance world operates.

Shortest Path Bridging, however, supports lightning fast convergence times. In testing, when the primary core switch was unplugged, more than 8,000 H.264 video feeds converged to the secondary path in less than a second. The same test was conducted with five leading VMS platforms with similar results: no live-view or recording ability was lost. In fact, the VMS platforms were not aware that any failure had occurred.

Unlike traditional networking technologies, Shortest Path Bridging will faultlessly keep both links from intermediate distribution frame (IDF) closets active and load balanced. Traditional networking technologies often shut down one of the links to prevent a network loop; the user is paying for redundant links but only using one at a time.

Leveraging Automation

The networking world is currently going through a major transformation, from white-box and bright-box technology to software-defined networking. With a wide and diverse range of applications driving specific networking needs, applications now communicate with software-defined networking controllers to establish required criteria.

The simplicity of Shortest Path Bridging, and the limited number of unique variables associated with it, has opened the door to automated switch deployment and configuration for the entire security industry.

While most software-defined networking is in the data center, this emerging technology is starting to shape the way the surveillance world operates. For greenfield installations and deployments where surveillance integrators control the IP space, automation has become a reality.

Networking needs are driven by the VMS function and network traffic profiles. Imagine a world in which security professionals can deploy optimized security networks through controlled single-line automation. In

other words, an integrator can take 20 switches for a given deployment and execute a single command on each switch.

Within seconds, the switch is configured and optimized to deliver video surveillance traffic in a unicast or multicast environment. What does this mean for the security industry? It means getting the network right the first time. Automated configurations remove the human element from surveillance network deployments and reduce repeated truck rolls to resolve network-related issues.

Taking Automation to the Next Level

From an integration standpoint, there are obvious benefits to automating network configuration and deployment. Can automation help manage an active surveillance network?

Several leading IP camera manufacturers are currently working on embedding Shortest Path Bridging "auto-attach" features into their cameras. This technology will allow secure communication, authentication, and provisioning for security devices. In other words, if the device supports auto-attach and is authenticated, the network switch port will be automatically programmed to meet the requirements of the security device.

Furthermore, any device that does not support auto-attach, or that is not authenticated, will lack the network programming to function. As a result, this type of automation acts as an enhanced level of security for devices that support the auto-attach feature.

A Better Way to Multicast

For many years, the security industry has been debating the need for multicast. The fundamental issue revolves around scaling resources for live-view. An IP camera is only capable of generating a limited number of high-resolution, high-frame rate streams before exhausting its resources.

In a unicast environment, pulling streams directly from the camera limits the number of viewers before failure occurs.

The proxy model sends a single high-resolution unicast stream to the recorder or archiver, then the proxies stream out for live-view from the server. Given the robust resources allocated to a typical server, this seems like a good solution, but it creates several potential problems.

Automated configurations remove the human element from surveillance network deployments and reduce repeated truck rolls to resolve network-related issues.

Performing the proxy function on the server induces latency, increases camera population time, and puts undue stress on the server or archiver. In testing, it has been shown that removing the proxy feature from the server dramatically reduces the saturation of local server resources and allows for a higher max bit rate by the server and its associated roles.

This means that removing the proxy feature will reduce the overall server hardware required to handle the incoming bit rate. With the proxy feature removed, the VMS platform must rely on

multicast streaming, directly from the cameras, to deliver the required number of live-views.

In the past, multicast networks were something to be feared and required a very high level of networking knowledge to be implemented properly. Times are changing, though. Automated deployment scripts can deploy multicast flawlessly without any of the complexity of the overlay model. Moreover, multicast over Shortest Path Bridging outperforms expensive core switches at a fraction of the cost.

Shortest Path Bridging for multicast has been deployed throughout the world and supports metro stations, city surveillance, and critical infrastructure. These deployments have ranged from 80 to 12,000 cameras while delivering a highly available multicast network on multiple VMS platforms, all while optimizing performance and efficiency.

Multicast networks for surveillance applications no longer need be feared or avoided. Shortest Path Bridging allows the deployment of multicast without the associated risks of overlay networking. Given the benefits of faster camera population, less latent PTZ control, fast convergence and reduced server hardware costs, the choice is clear. If a VMS supports multicast edge video delivery, it should be embraced. Sometimes, simpler is better. ■

Darren Giacomini (dgiacomini@bcdvideo.com) is director of networks for BCDVideo (www.bcdvideo.com).

It is paramount that the integrator understands your world and can assist with using technology to enhance safety and security while maintaining compliance.

Diagnosing Security Challenges

Developing the secure hospital of the future starts with planning and collaboration today

By Marianne Iannotta
Kratos Public Safety & Security Solutions

A hospital in America continues to be one of the most dangerous places to work. Health care organizations face a varied and constantly evolving threat landscape, from longstanding issues with workplace violence and infant abductions to more modern malicious activities such as cyberattacks and data breaches. Hospitals must be ready for anything that would disrupt their ability to provide care, jeopardize the safety of patients and staff, or damage the reputation of the health system. At the same time, they must remain in compliance or risk audits by regulatory bodies.

Some of the incidents that are happening today were unimaginable a few years ago, so it is no surprise that relying on older systems is limiting success in adapting to new challenges. Data is now obtained from multiple devices, including video management, computer-aided dispatch, mobile phones (and the cameras that reside within them), GPS tracking, mass notification, panic alarms, intrusion detection, and more. Protecting a hospital environment requires a vast number of sensors, but unifying multiple devices into one system to gain complete situational awareness remains a challenge. Therefore, identifying the best solution requires working with a team from both a technical and an operations background, and that includes physical security, data security, IT, and hospital operations. Furthermore, integration partners should have subject matter experts who are mindful of all relevant challenges and who can be a collaborative partner to other departments, such as risk management, privacy, IT, and human resources, among others. They should be a total solution provider, not a parts and pieces installer. Through a collaborative effort, hospitals can leverage technology to create the secure hospital of the future.

The Secure Hospital of the Future

What does the secure hospital of the future look like?

- It has enhanced campus security and provides an environment of care and comfort to patients, visitors and staff.
- It has reduced costs of claims and improved Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) scores.
- It has a centralized command and control center on one platform that is bidirectional in its communication.
- It has improved its operations and workflow, such as cross-department and cross-hospital coordination, with risk management, facilities and IT.
- It is using nonconventional means to enhance its environment of care. For example, some hospitals have placed cameras at the entrances of hallway bathrooms. In addition to providing a security benefit, the cameras count the number of people who enter

the restroom and, after a certain number, notify a cleaning crew.

- It is better at managing its devices and assets. Security has a record – an audit trail – of access to all controlled areas in the facility.
- Security relies on sound protocols and response procedures and has become more efficient and effective in deploying them.
- And, of course, it is in full compliance with regulations.

Assuming you embrace change in order to future-proof your hospital, physical security will converge to a virtual environment. Your secure hospital of the future continues to thrive in the midst of risk. Your security department is in lockstep with IT, its applications and its network. Your data is automatically aggregated by systems you have put in place. You have demonstrated cost savings, reduced space, and developed an efficient IT infrastructure. You have become the centerpiece of the hospital portfolio for infrastructure assessment and improvement. Not only are you *not* a cost center, you have decision-making authority because of the multiple levels of ROI that you demonstrate. Your peers appreciate having previously unobtainable data and you deliver a wealth of cross-functional value in the form of operational intelligence gathering. Like other department heads, your business processes are driven by policies that are based on regulations and industry best practices.

You are counted on because of the data points and sensors in the ceiling that were previously referred to only as cameras. They provide, among other things, information on improving and securing your infrastructure, reducing risk, streamlining workflow, and enhancing the quality of care. You provide a high degree of situational awareness to operational executives. You have seamless communications mediums, detailed protocols, and adequate coverage to protect your health system from any liability. You have the ability, training, and comfort to access any of these systems in order to identify incidents.

Some of the incidents that are happening today were unimaginable a few years ago, so it is no surprise that relying on older systems is limiting success in adapting to new challenges.

Your security officers and operators have one system that aggregates data from all of their previous screens. This system includes video surveillance, access control, social media, alarms, and geolocation systems to understand where an event is taking place. Not only does security staff have better information, they are more prepared with response protocols that are launched when an event is triggered. Management departments work closely with security to build a proactive partnership to

develop the hospital's safety and emergency response plans as the environment of care changes.

Failing to Prepare

What will happen if you do not prepare for the secure hospital of the future?

Physical security systems have converged to IT, but you continue to use siloed tools, leaving your team with multiple devices and monitors to manage. The alerts from all of these standalone systems require time and attention, and you realize that you are working for your technology instead of having your technology work for you. Your department continues to react, respond, and recover, losing millions of dollars in time, productivity, reimbursements, and employee turnover. You have submitted your budget, but your $250,000 request has been denied because the radiology department was able to demonstrate ROI after just four months for a $1 million machine.

You get hacked. Data thieves gained entry through the access control system because the security equipment has not kept pace with the technological progression of the rest of the hospital. Your patient and employee information has been exposed, and the news has made the cover page of peer-reviewed publications as an example of what goes wrong when security is not taken seriously. The Occupational Safety and Health Administration (OSHA) has cited you for violence committed against nurses in your emergency department and for not demonstrating any sort of improvement, staff comfort, or safety. You have gotten the attention of The Joint Commission and, despite an inspection not being due for another year, they will be showing up at your facility any day now. Staff morale is down and you struggle to recruit good talent. These challenges have negatively affected the quality of care and the hospital's HCAHPS scores reflect this.

So is not preparing really an option?

The Path Forward

At a minimum, three departments need to be included in the process of identifying security solutions: Risk, Finance, and IT. These three branches of governance should be data mining their non-recoverable costs. What costs could have been prevented? What is the risk and cost associated with doing nothing? How much can be captured by doing something? Demonstrate that your budget is obtained from a portion of the hospital savings that you have created through cross-department collaboration.

Identifying the best solution requires working with a team from both a technical and an operations background.

Risk

Risk includes things as varied as threats on social media to spending millions of dollars to have security officers watch patients one-on-one.

Why isn't there integrated social media monitoring? Why isn't visual monitoring set up like telemetry? Hospitals have been doing a 1-to-20 or even 1-to-30 patient ratio with physiologic monitoring for years. Yet only two hospitals in the United States have data showing

the millions of dollars in recoverable costs on payroll resulting from sitter utilization after implementing a camera monitoring system. That is two out of 5,724 hospitals in the nation. Save millions of non-recoverable payroll costs, invest a portion of that savings in a camera system, and write off the expenditure in capital equipment while maintaining a consistent and reliable approach to the new intensive monitoring equipment. Anytime you reduce risk, you reduce insurance premiums. Who pays your insurance bill? After implementation to improve the security of your infrastructure, how soon will the savings hit the bottom line? What else can be done to further reduce premiums?

Finance

Do you have an $800 non-recoverable cost that is showing up repeatedly? Most hospital systems in the country have a dollar amount for paying out claims without extensive inquiry. In one case, a single fraudulent incident turned into nine when the perpetrators realized that getting compensated by the hospital for a "lost wallet" was easy. It was not until the security director was notified of this that cameras were installed in the area where the incidents were supposedly taking place. While it may seem small, if a company has multiple facilities at which it is occurring, this security gap could quickly become expensive. Another major consideration is high dollar amount claims. These are the slip-and-falls that cost you millions of dollars because you have no evidence to support your defense. How much are legal fees costing your hospital for incidents that could have been dismissed if a video recording had been available?

IT

It behooves the security director to work with IT from the start. In short, if it's IP, it's IT. Collaboration should be exactly that: collaborative. The convergence of physical security systems, the pipeline for collecting, transferring, and storing data critical for daily operations, is a function of IT. However, IT generally is not capable of being proficient in every physical security technology, making the active participation of security in the process essential.

Physical security will converge to a virtual environment.

These are examples of components that should be prioritized to realize immediate operational and financial benefits. They can change a conversation with a CFO from "I need to get budgeted for this" to "Let me show you how much I'm saving you." It is win-win for everyone, including employees, who work in a safer environment and see that their safety and security is important to their employer.

Choosing a Partner

Whom do you trust to be an extension of your team, to be your systems integration partner? Integrators should be in it for the long haul. They should be your trainer and advisor and, quite often, your advocate and friend. It is paramount that the integrator understands your world and can assist with using technology to enhance safety and security while maintaining compliance. An integration partner and solution provider should stay on top of the latest trends and technology and should have relationships with the leading health care security organizations.

The core competencies of a reliable solution provider are:

- They are accurate in their assessments.
- They are current with where you should be and are aware of the technologies that are available.
- They are experts in demonstrating how security technology is moving beyond traditional security applications.
- They recognize that hospitals are different from other organizations and have their own set of regulatory agencies.
- They are unbiased and vendor-neutral.
- They recognize and communicate what is essential.
- They not only provide recommendations, they give you options based on timelines, time constraints, priorities, prices, etc.
- They provide solutions that are readily usable.
- They show immediate benefits and savings, such as demonstrating how to obtain quantifiable data to support security initiatives.
- There is no drama on the

backend, like erroneous invoices, manufacturer hiccups or inventory shortages.

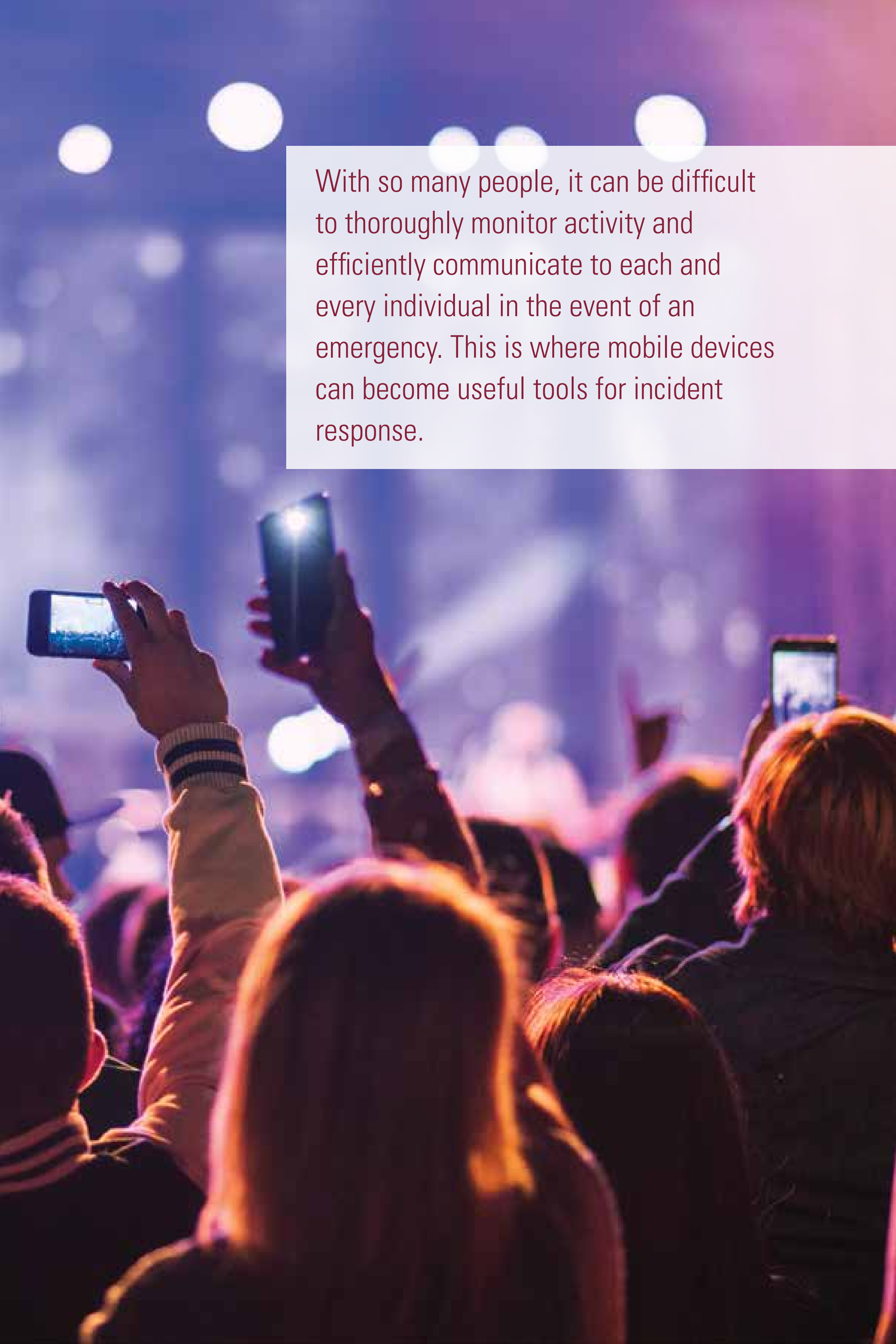
Now What?

Hospitals will not see any relief from the barrage of threats they currently face by being complacent. In fact, the challenges will probably only increase. Patient populations continue to grow, workplace violence is ever present, hackers are becoming more sophisticated (and health care data more valuable), and the opioid epidemic shows no signs of abating. But there is good news in this daunting scenario: Technology can help provide solutions. It is up to security directors, though, to start planning for the secure hospital of the future today. The convergence of physical and IT security offers insights and coordination that were not thought possible until recently. Leveraging this technology and the new processes and procedures that come along with it, will enhance organizations' ability to address these threats.

Change does not have to come all at once. Now is the time, though, to organize teams, present the possibilities and benefits, and begin to build out security systems. Integrator and manufacturer partners need to have a part in this and should be providing scalable technologies with an eye to a future holistic system. The best solution for right now (whether in terms of cost or technology) may not make sense in the long term and could set the whole effort back significantly. The industry has made tremendous strides in both technology and best practices. The path forward is there, and now is the time to take it. ■

Marianne Iannotta (marianne.iannotta@kratospss.com) is a hospital security specialist at Kratos Public Safety & Security Solutions (www.kratospss.com).

With so many people, it can be difficult to thoroughly monitor activity and efficiently communicate to each and every individual in the event of an emergency. This is where mobile devices can become useful tools for incident response.



Dialing Up Security

Smartphones can be an essential component of a mass notification system

By Jana Rankin
VuTeur

Smartphones permeate our lives. In fact, 91 percent of adults keep their smartphones within arm's reach, according to Morgan Stanley, and Daily Infographic reported that the average person looks at his or her phone approximately 110 times a day.

Consumers are clearly hooked on this multifaceted lifeline. In today's mobile culture, the rise of these devices has changed the communications landscape, offering more options for security companies to utilize technology to streamline operations through access control, two-way communications and – most importantly – emergency management and incident response.

The safety and security capabilities that are available keep increasing. Parents can now track their children through their phones; Amber and severe weather alerts are automatic; and surveillance camera footage can be streamed on the devices of security personnel. About three-fourths of cell owners have used their phones to get help in an emergency, according to the Pew Research Center, and many people use Twitter or Facebook, as well as other social media platforms, to locate or check in with friends and relatives during a crisis.

Specific sectors of public security, such as access control manufacturers and incident response software developers, have shifted to a more digital world. This has led to more streamlined responses in dangerous situations.

Real-Life Incidents Warrant Action

In 2007, a Virginia Tech student opened fire at the university, killing 32 people and wounding 17 others before killing himself. Last year, 49 people were killed by a gunman at Pulse nightclub in Orlando, Fla. And in May of this year, Manchester Arena in the United Kingdom was the site of a bombing that took the lives of 22 people and injured 116 after an Ariana Grande concert.

Expansive, high-capacity environments like these can easily become targets. Sprawling campuses and event venues are also vulnerable to a variety of other threats, such as severe weather and other natural disasters, making it critical to have an emergency preparedness plan in place. But with so many people, it can be difficult to thoroughly monitor activity and efficiently communicate to each and every individual in the event of an emergency. This is where mobile devices can become useful tools for incident response.

It is unlikely that security personnel could reach every person within a facility verbally, so a platform that uses an item almost every person already has can help facilitate a faster response.

Real-Time Location Services and Incident Response

The use of cell phones for incident response and emergency management is based on real-time location system (RTLS) technology, which is used to automatically identify and track the location of objects or

people in real time. This is usually done within a building or other enclosed area. It is like GPS, but for indoors. While GPS is able to track vehicles as they move across the globe, it is unable to track the hundreds – if not thousands – of devices that are often in a small space, such as an event venue or a busy airport facility. This is where RTLS becomes the best means by which to communicate location. RTLS technology has the ability to read wireless devices automatically and continuously, making it a better fit for security purposes.

Using smart devices that send a signal to a central monitoring platform through the facility's Wi-Fi connection, security officials can know where people are located within a specific area and can alert them in the event of an emergency without having to use an application. It is unlikely that security personnel could reach every person within a facility verbally, so a platform that uses an item almost every person already has can help facilitate a faster response.

RTLS technology is also well suited for supply chain management, health care, military and government, retail, recreation, and education. In terms of security, RTLS has a significant and emerging place in the market.

Emergency Preparedness Planning

The use of RTLS technology must be coupled with a comprehensive emergency management plan. To start, organizations must first identify and implement best practices for incident response, including:

- **Establishing internal communications –** Answering important questions, such as who will be responsible for sending messages and what technology will be used, is critically important.

- **Involving external stakeholders –** Establishing fluid partnerships between an organization and first responders before an incident occurs is vital. Determining who should be involved, how they should be notified and how information should be shared are among the factors that must be addressed.
- **Using technology –** Mass notification solutions allow organizations to send out both standardized and customized messages through a variety of methods. Determining the kind of technology that will be used, as well as establishing standard operating procedures when using the technology, will help augment emergency response.
- **Clearly defining involvement –** There needs to be a clearly defined chain of command within every organization that identifies who is responsible for communicating with each group of stakeholders, and how they are going to communicate with them. There should also be a backup plan in case of absences.
- **Tailoring messaging –** Because each and every event is different, strategies should be in place to respond accordingly. A bomb threat is much different than an active shooter incident or severe weather. Messages and their content need to reflect proper procedures.

While all of these best practices can be used together to formulate a comprehensive plan of action in the event of an emergency, the most important factor is to involve local law enforcement and fire department officials in any incident management planning. Not only do they need to understand what the specific emergency messaging and evacuation processes are for a particular business or institution, they also need to be familiarized with the ins and outs of the facilities themselves. This will likely include the locations of entrances and exits, surveillance cameras, and alarm triggers, as well as details of how lockdowns are implemented. All of this information can be combined to present a complete picture of a facility's response plan before it is needed. Failing to keep first responders in the loop can cause confusion during an emergency.

> The most important factor is to involve local law enforcement and fire department officials in any incident management planning.

Strengthening Collaboration with RTLS

The choice to implement a mass notification system is a large undertaking for security leaders, and it can be a major investment, which means ease of use, scalability and flexibility must be considered. Not only does RTLS technology work well in an emergency situation for communications between first responders and those experiencing the incident, but it can also be used on a routine basis.

For example, in a campus environment, administrators can communicate directly with faculty and students about an event or an upcoming closure. Retail locations can communicate promotions to customers on a regular basis, boosting marketing efforts and sales. Event venues and stadiums can communicate weather delays or other key developments that affect start times. And these are just a few of the innovative ways that smartphones can be used to streamline and enhance operations.

> Not only does RTLS technology work well in an emergency situation for communications between first responders and those experiencing the incident, but it can also be used on a routine basis.

The ongoing advancement and development of mass notification and communications systems continues to offer end users a wide range of options to improve their responses during emergencies. Being able to utilize existing location-based smartphone technology – integrated with access control, video surveillance, and alarm systems – improves an organization's ability to protect people and assets, while enhancing response and investigation capabilities. ■

Jana Rankin (jrankin@vuteur.com) is the CEO of VuTeur (www.vuteur.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:

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

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

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

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

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

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

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

securityindustry.org/techinsights

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