Physical Security's Tech Revolution

The physical security industry is facing an unprecedented opportunity to enhance security programs with emerging technologies.

Rapidly changing technology

Cost constraints

Compliance requirements

ASIS INTERNATIONAL
Advancing Security Worldwide®

SECURITY MANAGEMENT

How Emerging Technology will Revolutionize Enterprise Security and the Work Environment

Never in the history of the physical security industry have emerging technologies been poised to substantially impact the delivery of security programs and services on campus environments as much as they are now.

By William Plante

Never in the history of the physical security industry have emerging technologies been poised to substantially impact the delivery of security programs and services on campus environments as much as they are now.

The adoption of artificial intelligence (AI) and machine learning (ML) in the video management sector is just one small example of technology increasing confidence in the system's abilities and measurably improving returns on end user investments. But that's only the beginning. The likes of AI-driven humanoid robots and aerial drones that seamlessly integrate with physical security systems, all managed within an interoperable metaverse are just over the horizon. Augmented and virtualized reality (AR and VR) environments coupled with a multiple-domain intelligence platform will be used to support richer and more effective end-user experiences and collaboration for better security outcomes.

The COVID-19 pandemic forced many enterprises to adopt work-from-home and modified workplace strategies, and it has compelled technology companies to research and pursue the development of solutions that facilitate our new ways of living and working. With such purpose-driven change, the security industry will ultimately benefit—as long as we remain dedicated to staying ahead of the curve.

However, a word of caution. The emerging technologies that are taking root in the enterprise landscape represent a once-in-a-lifetime quantum leap in value to the security industry and corporate adopters. Emerging technologies speak to the corporation's expectations that systems, including security, will provide incremental value via usable data and information, as well as visualization, analytics, and decision-making support. Therefore, one does not simply adopt emerging security technology. Successful organizations should develop use cases that align with business objectives to support a case for adopting emerging technologies. They should do this by implementing proof-of-concept trials that demonstrate the technologies' usefulness and other similar activities.

ARTIFICIALLY INTELLIGENT AERIAL DRONES AND HUMANOID ROBOTS

The computer scientist Cal Newport has written extensively about workplace and worker impacts of emerging technologies. In particular, he describes the division of knowledge and non-knowledge workers and notes that emerging technologies will more adversely affect non-knowledge workers.

The implication for our industry is clear: Adopting drones and robots will require a new kind of organization beyond people who simply monitor physical security sys-

tems or guards that perform routine patrols. Many chief security officers are keenly aware that the security guard industry has long been experiencing a labor shortage that leaves it struggling to fill its ranks, creating service gaps—a trend that is anticipated to continue.

Successful organizations should develop use cases that align with business objectives to support a case for adopting emerging technologies.

For many organizations, security operations center (SOC) operators are primarily tasked with acting as alarm acknowledgers and dispatchers with limited analytical activity requirements. Aerial drones and robots are already deployed to both supplement and, in some instances, fill in for human guards. AI-enabled drones and robots can perform a wide range of guarding tasks in three modes: Human-operated, AI-operated, or a hybrid of both. Notably, the AI that drives drones and robots is developing an ever-increasing sophistication and capability due to machine learning and the fine tuning of the data sets that train these machines.

METAVERSE INTELLIGENCE PLATFORM

The term "metaverse" suddenly jumped to prominence when, in October 2021, CEO Mark Zuckerberg announced that Facebook would become Meta. But virtual, augmented, and mixed reality has been available in various ways long before this, primarily to video gamers and training applications.

While still nascent, a metaverse interoperable security environment is not too far into the future, and its uses and benefits are compelling. For example, virtualized SOCs with a highly interactive operator and user environment

can result in optimized operations and outcomes, while highly integrated AI-driven video and access systems can present an operator with a digital twin of a building overlayed with access alarms and responding resources—whether they be humans or robots.

KEEPING IT REAL

While much of this sounds like the stuff of science fiction, the real question is how can these developments be applied in a corporate campus? Here are just two examples of how emerging technology will revolutionize security and the workplace.

Let's consider a large manufacturing campus that requires 24/7 operations with excessive valuable raw materials stored in trailers near the plant. The trailers should only be accessed during the dayshift. The security program includes an anomaly-detecting AI that evaluates the access control system, an AI video system that monitors the area around trailers, and an aerial drone that is used to patrol the perimeter routinely. The system detects an access anomaly when a contractor with 24/7 access enters the property using a non-company pickup truck, which is observed via the license plate reader. The contactor parks near the trailer, which trips the AI video and begins real-time recording. The security patrol drone is diverted from the perimeter patrol to investigate the area, and the drone captures video of two persons moving raw materials onto his truck. The system operator is able to determine that the person isn't the credential holder and that the truck isn't authorized. It then is easily able to determine a workplace theft is in progress and calls the police. The security team never needs to confront the thieves directly, and the police have knowledge of the situation they're responding to.

In another scenario, a company has implemented a work-from-home policy for most of its employees, including its security operations center program. The company can adopt virtualized technologies by rearchitecting the hosting infrastructure toward a cloud-based solution that incorporates AI access and video systems. This redesign also includes a metaverse representation of the offices and online staff, and the deployment of humanoid robots for on-premises monitoring and response. The SOC operator can perform a remote security patrol on one robot while monitoring critical systems in the headset. When the intrusion alarm is set off in a far corner of the building, the operator can seamlessly transfer his or her "presence" from one robot to the nearer robot as it responds to the alarm.

COVID-19 has introduced a hybrid workplace strategy, with organizations enacting policies that span from work-from-home, to return-to-work, or a blend of both. The effects of COVID-19 will be with us for a long while yet, and it has compelled companies to rethink their security strategies and program delivery.

Emerging technology—including AI-driven systems, robots and drones, and broader applications—will morph and adapt to the new workplace. And thoughtful planning will be a necessary to create an effective process for moving the security program into the next-generation corporate campus environment.

WILLIAM PLANTE, IS DIRECTOR, CONSULTING & STRATEGIC DEVELOPMENT, ENTERPRISE SECURITY RISK GROUP, AT ADT COMMERCIAL. PLANTE HAS WORKED IN THE CONSULTING FIELD FOR 15 YEARS, LEADING COMPLEX TECHNOLOGY AND ENTERPRISE RISK PROJECTS. HE HAS ALSO BEEN A CSO AND IT CONTINUITY DIRECTOR FOR TWO HIGH-TECHNOLOGY FIRMS.

How Ticketing Technology Securely Streamlined the World Cup Fan Experience

Football fans from across the globe traveled to Qatar to attend the 2022 FIFA World Cup. Here's how HID developed a solution to ensure the integrity of their tickets and an efficient entry process to matches.

By Cesare Paciello

Every four years, the FIFA World Cup shines as one of the largest and most popular sporting events in the world. The 2022 version was no exception, spanning eight stadiums across Qatar, with more than 1.4 million visitors attending matches. The eight newly constructed stadiums hosted 64 games and 32 participating teams, with capacities between 44,000 and 89,000 spectators for each game.

With an event garnering this much demand, one of the biggest challenges for FIFA was managing the ticketing experience. Due to the sheer volume of ticketholders and the frequency of matches, it was important to have a technology that would work effectively and securely.

TICKETING 101

When most fans purchased their World Cup tickets for the 2022 tournament, they received them as mobile tickets to

be downloaded via the Official FIFA World Cup 2022 mobile ticketing app. Ticketholders installed the app on their smartphone, created a FIFA Ticketing account using their personal data and email address used for the ticket purchase, confirmed their email address, and then had access to the tickets they purchased.

In some instances, fans bought their tickets at FIFA ticketing centers in Qatar—part of the Last-Minute sales phase—and received paper tickets in person.

Knowing that counterfeit tickets have historically been a problem at sporting events of this magnitude, the sale of illicit tickets was a concern for FIFA.

To combat counterfeit sales, HID delivered a smart ticket with multiple security features—including an RFID inlay manufactured with special security papers.

To help address these worries for a third World Cup, HID provided unique RAIN RFID technology to facilitate identity verification in the ticketing process. RFID differs from traditional barcoded tickets, which can more easily be counterfeited, by transmitting the unique identity of a ticket and its holder via radio waves. Unlike barcode readers, RFID scanners do not need a line of sight with the RFID chips

To combat counterfeit sales, HID delivered a smart ticket with multiple security features—including an RFID inlay manufactured with special security papers. The data stored in each ticket's RFID chip was also encrypted and digitally signed.

The RFID tickets were made of three layers: the top, middle, and bottom layer. The top layer consisted of thermal paper that is used for variable data and personalization, including UV ink printing in two colors. This is in addition to a customized 2D hologram and micro-text that

were embedded in the ticket. The middle layer consisted of an RFID inlay chip. The third layer was made of security paper—similar to the paper used for bank notes production—which includes physical objects that are mixed into the paper pulp during the production process.

HID has been producing these RFID tickets for three consecutive events for FIFA World Cup, delivering approximately 2 million paper tickets at the 2022 tournament alone.

STREAMLINING ACCESS

Having a highly secured ticket meant that attendees could simply tap their tickets to a reader to gain access to an event, speeding up admissions throughout the duration of the World Cup.

HID was also tasked to provide an outer-perimeter access control layer for each stadium and across Qatar.

To support this, several thousand handheld high-frequency RFID readers were provided by HID so that staff could scan all visitors entering the stadiums and training fields, whether carrying an RFID/mobile ticket, RFID paper ticket, or RFID/digital Hayya card.

Once a visitor approached a venue entrance, event officials scanned each ticket's tag. Once the ID was authenticated, it automatically displayed approval on the handheld reader so that the ticketholder was permitted to enter the stadium. This system allowed fake tickets to be identified, preventing individuals from entering the stadiums under false pretenses. The system also allowed the officials to obtain a full view of people entering and exiting the facility, and better manage traffic flow. Once the ticketholders were inside the stadium, they were allowed to roam freely.

In addition, 200 gates were embedded with a new, patent-pending ultra high frequency (UHF) booster technology developed by HID to manage the stadium exit.

As part of the project, HID also provided a personalization solution for the secure tickets, including self-service kiosks for media seat assignment tickets, cabinets for tickets, instant issuing with special printers for on-the-go ticket personalization and on-site support during each match.

An accompanying Event Management Platform (EMP) provided real-time data and reporting through several user-friendly dashboards, which helped security officials and event organizers remotely monitor and manage everything from the number of attendees at each entry and exit point to media credentialing and crowd control.

Having real-time data of when ticket holders are going in and out of the perimeter is crucial for event organizers to ensure the best possible experience for fans, as well as obtain intelligence as to where a particular gate needs more attention in terms of crowd control and emergency evacuation.

CESARE PACIELLO IS VICE PRESIDENT OF EVENTS AND MOBILITY SOLUTIONS, HID. HE JOINED HID IN DECEMBER 2017 TO APPLY HIS DECADES OF EXPERIENCE IN THE DIGITAL SECURITY, IDENTITY, TICKETING, AND TRANSPORTATION INDUSTRY TOWARD DRIVING SEGMENT GROWTH AND SOLUTIONS DEVELOPMENT. PACIELLO ALSO HAS SERVED AS VICE PRESIDENT OF EUROPEAN, MIDDLE EAST, AND AFRICAN (EMEA) SALES FOR ARJO SYSTEMS SINCE FEBRUARY 2015. PRIOR TO THIS, HE WORKED FOR ARJOWIGGINS SECURITY, ALSO IN EXECUTIVE AND MANAGEMENT POSITIONS OVERSEEING TICKETING AND TRANSPORTATION PRODUCTS AND SERVICES SOLUTIONS. PACIELLO GRADUATED IN ECONOMY AND AT THE UNIVERSITÀ DEGLI STUDI DI SALERNO AND THEN FOLLOWED INSTEAD EXECUTIVE PROGRAMMES IN SINGAPORE AND INFRANCE (INSTEAD) AND IN MILAN AT 24 ORE BUSINESS SCHOOL. FOR MORE INFORMATION, GO TO: HTTPS://WWW.HIDGLOBAL.COM/SOLUTIONS/SPORTS-AND-EVENT-MANAGEMENT, OR EMAIL MARKETING@HIDGLOBAL.COM

SECURITY MANAGEMENT

How Technology Helps Multi-Housing Community Managers Work with the Fire Department to Improve Incident Response

Opportunity Home San Antonio recently adopted an automated notification system that alerts staff to fires in real-time.

By Domingo Ibarra

Fires are a significant problem, devastating people and property. In just 2 minutes, a fire can become life-threatening. Within 5 minutes, an entire residential structure can be fully engulfed in flames.

Prior to implementing an automated technological solution, community managers at multi-housing communities would often hear about a fire at their property in the news or when they next reported to work.

Most multi-housing organizations cannot maintain a continuous state of alertness, especially during late or early morning hours when staff is not on duty. Fire departments cannot contact specific managers or on-call maintenance technicians that are on an on-call rotation schedule.

During fire events, vulnerable residents—the elderly and disabled—can be left to fend for themselves outside of the building until management is notified. This becomes an even more tenuous situation when there is inclement weather.

OUR SOLUTION

Opportunity Home San Antonio provides affordable housing, social services, and assistance to more than 57,000 children, adults, and seniors in San Antonio, Texas. It recently adopted an automated notification system that notifies staff about fires in real-time.

The Fire Incident Response Event (FIRE) A.L.E.R.T. (Automated Location - Emergency Response to Threats) was established by working with the San Antonio Fire Department (SAFD) and its Computer Aided Dispatch (CAD) technology.

The Opportunity Home Policy & Planning Department provides an updated list of all the multi-housing communities to the City of San Antonio (CoSA) Public Safety GIS (PSGIS) group. All of the addresses are entered by PSGIS into the CoSA CAD system.

The automated system allows staff to track incidents and gauge the effectiveness of the response.

Now, when SAFD receives a call for service to an Opportunity Home property, this triggers the notification system to alert on-call managers. These alerts are sent by SAFD to Opportunity Home via email, which are automatically converted to SMS text messages, using a gateway service, that are sent to cell phones assigned to maintenance technicians and supporting Opportunity Home departments. When certain cell phone carriers began blocking SMS text messages when they suspected them to be spam, Opportunity Home upgraded its cell phone service to an enterprise product that has a minimal cost for monthly SMS text messages so our automated services will function without interruption. Management now has a continuous state of alertness with the help of this technology.

There are 47 categories where management receives an automated alert. These include appliance fire, arson investigation, bombs, brush fires, unauthorized burns, electrical, electrocutions, explosions, extinguished fires, fire alarms, gas leaks, high-rise fires, motor vehicle collision (on property), odor of smoke, smoke investigation, structure collapse, suspicious package, vehicle fire, hazardous material, and various others. The technology allows staff to respond to any crisis immediately and contemporaneously with SAFD. An example of this in action is when there is an appliance fire that renders the unit uninhabitable, our staff is alerted and transfers the resident to a vacant unit or coordinates a temporary stay at a hotel.

SAFD responds to tens-of-thousands of calls for service, many of which are false alarms. Both SAFD and Opportunity Home saw the opportunity for improved public safety collaboration—not just for responding to actual structure fires, but also addressing fire prevention initiatives and reducing the rate of false alarms.

The automated system allows staff to track incidents and gauge the effectiveness of the response towards improved detection and prioritization of actual emergencies. The operational component also allows the actual response team to go to the site of the fire in a timely manner.

The most important aspect of this system is the opportunity to learn from an incident to be better prepared for future incidents. The automated correlation facilitates various departments, previously missing from an organizational context, to allow management response teams to deploy an immediate infrastructure that supports all the logistics of response in a timely manner. Combining detection, prevention, and response reduces the time necessary to accomplish all tasks associated with a fire response, or elevator rescue, to properly follow-up and

document each of the various roles and responsibilities for the various departments.

The automated technology facilitates a holistic review of our incident response processes to find the areas where we could engage in critical thought and problem-solving, and provide immediate relief for residents to minimize expenses and damage associated with fires.

THE RESULTS

In February 2023, this system was put to the test when a fire broke out in a third-floor unit of an Opportunity Home community. The fire displaced more than 70 residents. Staff was able to respond to the location in a timely manner to coordinate the transportation of 51 residents to a local hotel and helped 19 residents who opted to make arrangements to stay with family or friends. Staff worked with the American Red Cross to assist with providing clothing, toiletries, Meals on Wheels, snacks, and financial assistance. Staff also helped with the delivery of medications to each of the displaced residents.

The most important aspect of this system is the opportunity to learn from an incident to be better prepared for future incidents.

The result of the program with SAFD was improved efficiency and effectiveness of management's administrative operations to address immediate needs of our residents when there is a fire. Some of these needs include obtaining a clean change of clothing, coordinating relatives that residents can stay with, obtaining a hotel for those who have no local relatives, and working with the American Red Cross to provide additional support.

Staff also coordinates ready-to-eat meals and hygiene kits, including new toothbrushes, soap and washcloths. Babies need diapers and formula in addition to clothes, while the elderly may need their medications. If the family has pets, staff helps them obtain shelter and food for them.

A further success of the program is that Opportunity Home is now able to reduce the amount of overtime previously paid to staff for responding to false alarms.

When the automated fire alert is received, staff conduct an immediate "Fire Alert Triage." Staff is directed to the SAFD Active Fire online page to monitor the call in real time. Staff also listens to the SAFD radio traffic via a telephone app to obtain updates on the status of the fire alert to verify if it is a false alarm, or an actual emergency that requires staff to deploy on-call staff. By only responding to actual emergencies, management is able to reduce overtime costs and improve the delivery of services. This correlation of details and placing context to actual emergencies allows staff to identify the alerts that constitute a real threat.

The fire alerts also help management, and our Risk Management Department, coordinate with contracted vendors to initiate the remediation process, as well as filing claims with insurance carriers.

This technology introduced a new set of organizational improvements to address challenges and incorporate automation.

Phase 1. Outline the steps to successfully respond to an incident, including incident qualification, triage, investigation, containment, notification, and post-hoc evaluation.

Phase 2. The tools and processes associated with the automation includes maintaining spreadsheets and doc-

umentsthat are shared between management and various departments. When we experience a few incidents a month, this proves very beneficial. The spreadsheets are used to track the location of each fire alert, what caused the fire, and the number of false alarms, which then allows staff to evaluate which communities need additional fire drills or fire warden training. It also helps staff plan for long-term capital improvements, such as when a fire panel needs to be repaired or replaced, as well as smoke detectors or other fire sensors.

These sheets allow staff to produce annual reports. During 2022, we received 836 fire alerts, which was evaluated with the previous year's totals, as well as how staff responded, to help identify areas for improvement.

When a large incident, such as a structure fire occurs, staff is able to respond to the location and create an interactive document where each specific department (Management, Security, Risk Management, Finance, etc.) is able to document their activities in real-time. This helps staff conduct an after-action review of all activities, which aids our emergency management planning and protocols.

Phase 3. The automated fire alerts enhance the maturity curve, and the orchestration or administrative processes are combined with this automation. Automation helps assess the impact of a threat, as well as the impact of the environment that initiated the threat. The automation allows staff to keep track of any patterns where repeated calls for service from SAFD could lead to have what has been referred to as "false alarm fatigue." When residents no longer have faith in a system and fail to respond appropriately to the alarm, this denigrates their confidence in the fire alarms. Staff works closely with the SAFD Fire Prevention Unit to address these types of issues by work-

ing with our staff to schedule "Safety Socials" to allow residents to ask questions and receive additional information about fire safety.

Notifying stakeholders, assigning incidents, and enriching data with context is a force multiplier that helps speed up the associated responses from each department. The actual containment of the fire rests with the SAFD, but the associated management of data frequently requires a well-coordinated effort to address fire prevention, detection, mitigation, and recovery.

DOMINGO IBARRA IS THE DIRECTOR OF SECURITY FOR OPPORTUNITY HOME SAN ANTONIO. HE IS RESPONSIBLE FOR MANAGING, COORDINATING, AND DIRECTING THE ACTIVITIES OF AN AGENCYWIDE ADVANCED SECURITY MANAGEMENT PROGRAM. IBARRA PREVIOUSLY SERVED AS CHIEF OF POLICE FOR MAGNOLIA, TEXAS, AND CEO FOR THE POLICE OFFICERS ASSOCIATION IN CORPUS CHRISTI, TEXAS.

Top 10 Best Practices for Security Grant Writing

Researching and writing grants can be time-consuming, stressful, confusing, and, well, boring. That's why we've put together a list of the top 10 best practices for grant-writing in the security industry to make sure your time is spent efficiently.

By Sonya Richmond

If you want to put your finger on the pulse of society, to identify where the real needs and challenges of today exist, the grants ecosystem can serve as a fantastic bellwether. Grants exist to meet public needs. This is why the groundswell of new funding opportunities in the United States for response-oriented security threats is a bittersweet development for people operating in the security environment.

On the one hand, the ever-growing list of grant opportunities in the security industry represents great opportunity for communities and security vendors. On the other, it is a sobering recognition of the increasing threat facing schools, municipalities, and the United States as a whole. Security professionals know that we can leverage this good to help address the bad, and funding exists today for qualified schools to obtain security solutions like access control systems, video surveillance, and even gunshot detection technology.

If you're only just learning about the grants ecosystem, don't worry, you're not alone! Every day, we work with organizations that have never before leveraged the grants ecosystem. Researching and writing grants can be time-consuming, stressful, confusing, and, well, boring. That's why we've put together a list of the top 10 best practices for grant-writing in the security industry to make sure your time is spent efficiently and (hopefully) to positive effect.

Read the fine print. Always. Every grant will include "eligibility requirements" in its request for proposals. Make sure you read these requirements carefully, because they will not only indicate whether or not you can apply, but also give hints as to if you can be competitive.

Research past awardees. Usually, grant-makers will not say the exact kind of institution they expect to fund. But you can glean this with a quick look at past awardees. If all 10 of last year's awardees were private colleges, and you're a fire department, you might reconsider applying—even if you are technically eligible.

You probably didn't pull a wheelie your first time learning to ride a bicycle. Grant-writing won't be any different.

Utilize letters of support. An investment in security for your organization is an investment in the safety and security of your whole community. The best way to show this—and bolster your application—is to collect and affix formal letters of support from organizational representatives, legislative leaders, and partners in your community.

Conduct a formal threat assessment. You know that your institution needs an improved security posture, but

quite frankly, you're a bit biased. At least, that's how you'll be seen by grant makers. That's why a formal threat assessment by your local police department is an important, credible, and unbiased means of proving your need without relying on your own perspective alone. There are public resources available, too, such as this one from SchoolSecurity.gov.

Listen to the experts. If you're a mid-sized to large organization, you probably have an in-house development, grants, or fundraising department. Meet with them. They are constantly in search of high-need projects for your organization and can assist you in the grants search. If you don't have an in-house department, you still may have coworkers, board members, or partners with grant experience. Ask around—you might be surprised.

Set expectations. You probably didn't pull a wheelie your first time learning to ride a bicycle. Grant-writing won't be any different. Regardless of the grant you choose, there are going to be a lot of competitive applicants, many of whom are applying for their second, third, or even fourth year in a row. The grants ecosystem is dependent on perseverance, and most funded projects are not first-time applicants with no history of partnership.

Grant writing is a skill. Cultivate it. There is virtually no industry, function, role, or circumstance in which a background in grant-writing and research will not be an advantage. Virtually every organization in the United States with more than 100 employees is—to some extent—leveraging or contemplating leveraging state, federal, and local funding opportunities. The time you spend learning about the grants ecosystem is not acute or temporal; it will be an asset of great value for the rest of your career.

Understand your match. "Match" is the amount of funds your organization is required to obligate toward the total

project/equipment budget. Most grant opportunities will indicate if they have match requirements and, if so, what percentage match is expected. Even for grant opportunities that do not have a match requirement, offering a small match as "skin in the game" can set your application apart and demonstrate your organization's commitment to the work in question.

Don't neglect leadership. Grants are, at their core, contractual agreements. In submitting a grant application, you are committing your organization to a set of activities and reporting requirements should you be funded. Accordingly, make sure to involve necessary leadership in finance, operations, and other executive functions to gain not only their approval, but their support for the application.

Don't be afraid to ask for help. Whether in-house or out-of-house, there are countless resources to support you in the grants process. Don't be afraid to ask for help.

SONYA RICHMOND IS THE FOUNDER OF SONICK GROUP, SHOOTER DETECTION SYSTEMS' EXCLUSIVE GRANTS PARTNER. SONICK GROUP IS CONTRACTED BY SDS TO ASSIST PROSPECTIVE CLIENTS IN THE GRANTS PROCESS. THIS ARTICLE IS NOT LEGAL OR FINANCIAL ADVICE. MAKE SURE TO FOLLOW ALL STATE, FEDERAL, AND LOCAL REGULATIONS IN RESEARCHING, SUBMITTING, AND ADMINISTERING ALL GRANTS.

Building and Defending a Plan for Preventative Maintenance

Preventative or routine maintenance is often the last thing thought about within the security industry after a project has been delivered or during the design phase. However, the single most important facet to making sure the delivered security system is functional and useable throughout the life of the site.

By Andrew Bugeja

If you didn't brush your teeth for a year and then went to the dentist, it would most likely start with some short-term pain in the lead-up and then result in having a few fillings when it's time to sit in the chair.

The same logic applies to maintenance of electronic security assets. Uncleaned cameras, for example, may display poor images. Operationally, this isn't great for live monitoring, but post-incident recorded footage would be practically useless.

When talking about electronic security though, we aren't just talking about keeping things clean. Often there are multiple devices ranging across different systems and potentially multiple sites that require customized approaches, depending on the technology and its priority to the organization.

Preventative or routine maintenance is often the last thing thought about within the security industry after a project has been delivered or during the design phase. It is, however, the single most important facet to making sure the delivered security system is functional and useable throughout the life of the site.

Adhering to basic principles when developing a preventative maintenance plan can not only lead to greater results on smaller sites, but it also means the approach to larger sites is well considered and effective.

The disappointing question around this topic within the security industry is typically, "Is maintenance being completed?" rather than "Is maintenance being completed to a high level of efficacy?"

The reasons for it not being completed at all often comes down to a premature conclusion of budget vs risk. In lieu of a fully considered approach, some organizations will swing towards a failure-based, reactive approach toward electronic security system upkeep, delaying the generation of a meaningful plan and engagement of a security maintenance contractor. Delaying for long periods of time, however, can lead to faults going unnoticed and snowballing to unmanageable levels.

Adhering to basic principles when developing a preventative maintenance plan can not only lead to greater results on smaller sites

In every case, security system upkeep should include a preventative maintenance plan (PMP) being in place to capture the basic principles and ensure a risk assessment has been completed. A result of this more thought-out approach may potentially even be keeping maintenance ac-

tivities at a lesser frequency to meet budgetary constraints.

Creating a good PMP requires several key elements to ensure the plan meets the organization's needs and that it can be defended in annual budget processes.

ASSETS

Knowing what is onsite and how those assets relate to each other operationally forms the basis for what needs to be done and when.

Assets are not limited to hardware items, and this inventory should include software and firmware which forms part of the overall security system. Given the steady increase in cybersecurity breaches and incidents, the importance of these upgrades can't be understated.

Some sites will have the luxury of generating this information during the core project delivery. Or for legacy or brownfield sites, this could involve potentially collating and verifying old and new data.

Asset lists should not be left to stagnate. Any removals or additions after the creation of the PMP should be captured to ensure the system is maintained in line with the existing plan.

ASSESSMENTS

Once the assets are known, a risk assessment can be made on the following:

Probability of deterioration/failure. This relates to the likelihood of the asset entering a state of ineffectiveness, and it can include external influences such as environment, human factors such as malicious damage, and internal factors such as asset type or asset quality.

Even within a security system where fit-for-purpose equipment has been purchased, an external camera installed in a dusty area may require more frequent cleaning than others.

Rate of deterioration/failure. This consideration relates to the time it takes an asset to become ineffective. Usage of an asset may determine this, such as backup batteries in a security system panel where the site's main power frequently drops out.

Impact of failure. The impact of an asset failure will strongly steer the requirements for preventative maintenance on security system assets because the impacts are often related to operational ability. If compromised, this can impact the safety of those on the site. The impact of a wireless duress alarm failure in the event of an emergency could be catastrophic.

Inversely, the impact of one camera being dirty where another camera may have an overlapping field of view may not affect the site's immediate operational ability.

TRIGGERS

Triggers define the "when" for maintenance activities. These triggers can be based on time, usage, or condition, or maintenance can be triggered manually.

The type of trigger used to initiate a maintenance activity within a preventative maintenance plan will be relative to the risk of failure of the asset.

Within preventative maintenance plans spanning long periods of time, pre-determined meantime between failure (MTBF) times may be applied to assets and used to schedule preventative maintenance activities such as life-cycling. Consideration should be given to the specific environment in which the asset is located as this may influence the probability of deterioration/failure.

For example, a wireless duress transmitter in a high-risk environment might be tested frequently while also having its batteries replaced well before the scheduled MTBF time to eliminate any risk of failure.

PROCEDURES

Procedures should primarily be designed to do two core things: test operational functionality of the system and undertake tasks to renew or refresh capability. The level of detail used on tests and tasks will be directly related to the assessment of the site and intertwined with the triggers.

For example, within an intruder alarm system, procedures may include testing all required alarms for devices while also cleaning and ensuring sensors are free from dust, dirt, or insect infestation.

SOFTWARE MAINTENANCE

In a constantly evolving industry, nearly all systems within the electronic security world are software-based.

Software upgrades solely servicing the introduction of new or improved features from suppliers are a thing of the past. Cybersecurity is highlighted constantly in today's technology landscape, and vulnerabilities are frequently found and patched in software releases. Updates also provide further stability as bugs are identified and fixed.

This should not only be a consideration for the security software itself but also for the infrastructure that runs the software. This could include firmware or operating software updates.

Keeping up to date with software upgrades also ensures newer replacement end devices are compatible. In some unfortunate cases, sites left not updated face challenges finding devices compatible with older software.

A risk-averse approach to software upgrade management may include an "N minus 1" approach, which means using the version from before the latest release. Its intent is to prevent downtime possibly related to any yet-to-be-discovered bugs in the latest release. While a consideration, this may not be the best approach if new features of a release are required.

LIFE-CYCLING

Life-cycling is the replacement of assets before they have failed. When considering life-cycling, it is important to refer to the PMP's triggers and risk assessment to determine how this will be undertaken. In relation to a security system's assets, this could be as simple as replacing a battery or replacing an entire system's end devices or headend infrastructure.

Due to the cost involved with replacing items, more cost-effective, condition-based triggers can used, or in some cases a trigger may be failure-based. Within environments where risk of failure can equate to large financial impacts or risk to a person's wellbeing, replacing equipment before failure is often a small price to pay.

Risk of outage should not be the only consideration in planning to life-cycle devices or systems.

The advancement of technology in an ever-changing industry is often a major reason for life-cycling assets.

A constant evolution of the site and its capability throughout time, if planned, can be cost effective and a manageable way of keeping up to date with the advantages of modern tech.

REPORTING

The product of the procedures and how it's communicated to the end client is the most important piece of the puzzle. A well laid PMP with great procedures that identifies faults only to be hidden within a report emailed or uploaded within an asset delivery system is not a functional mechanism—it is a considerable failure.

This communication should be relayed to the end user in a way that allows live feedback and questions to be asked, such as a meeting or face-to-face delivery. This live format allows a more consultative approach to the delivery and

will often inform decisions immediately on actions from the report findings.

Communication in this consultative form also creates a forum for review of the system as a whole, its effectiveness, and how it is adapting to the possible changing environment it services.

Reports generated throughout preventative maintenance can be presented by security managers to stakeholders to describe the health and compliance of the businesses security system. These reports can identify any faults and subsequent rectifications while highlighting the potential savings of capturing potential failures before they turn into incidents.

EMERGING TRENDS AND THE FUTURE OF PREVENTATIVE MAINTENANCE

Development of how preventative activities are generated, managed, and delivered has a very bright future and we only have other industries to look at to get an insight into what lies over the horizon. Some of the forementioned triggers and actions may already be implemented within existing software, but wider usage and implementation may become more prevalent in the future.

A commonality between some of these trends is that changes relate to how preventative maintenance activities trigger. This could mean automating or removing the trigger altogether via automation.

STREAMLINED UPGRADE PROCESSES

The requirement to upgrade software and device firmware is becoming commonplace among security systems and their devices.

More specifically the delivery method of these updates is constantly evolving. Manufacturers are bringing in a suite

of tools to not only smooth out the process of upgrades, but to also automate and time that process to reduce or eliminate downtime to due upgrades.

DATA COLLECTION AND USAGE

Collection and the use of data from a security system can be used to more accurately determine the MTBF and also act as a trigger for maintenance.

For example, a door that is used more than another could be triggered for maintenance activities earlier.

ANALYTICS

The analysis of inputs or sensors on items can be used to trigger maintenance before the item's planned interval-based trigger.

Due to the cost involved with replacing items, more cost-effective, condition-based triggers can used, or in some cases a trigger may be failure-based.

A great example of this seen outside the security industry is the use of Amazon's sensors within conveyor belt systems throughout the company's fulfilment centers. Sensor data is analyzed to determine if certain parts may be close to failure, allowing replacement of that part during scheduled downtime rather than knocking productivity offline when the belt breaks down, VentureBeat reported.

INTEGRATIONS

Mainly focused within the reactive service domain, integrations between security systems and service management interfaces could be used to more easily manually

trigger maintenance activities based on an operator's real-time analysis of the system's condition.

Other things such as the scheduling, coordination, and management of maintenance activities could be completed and easily tracked by both maintenance provider and end user.

Overall, consideration must be made when creating a PMP to balance the risk of failure against the cost involved with a comprehensive maintenance plan.

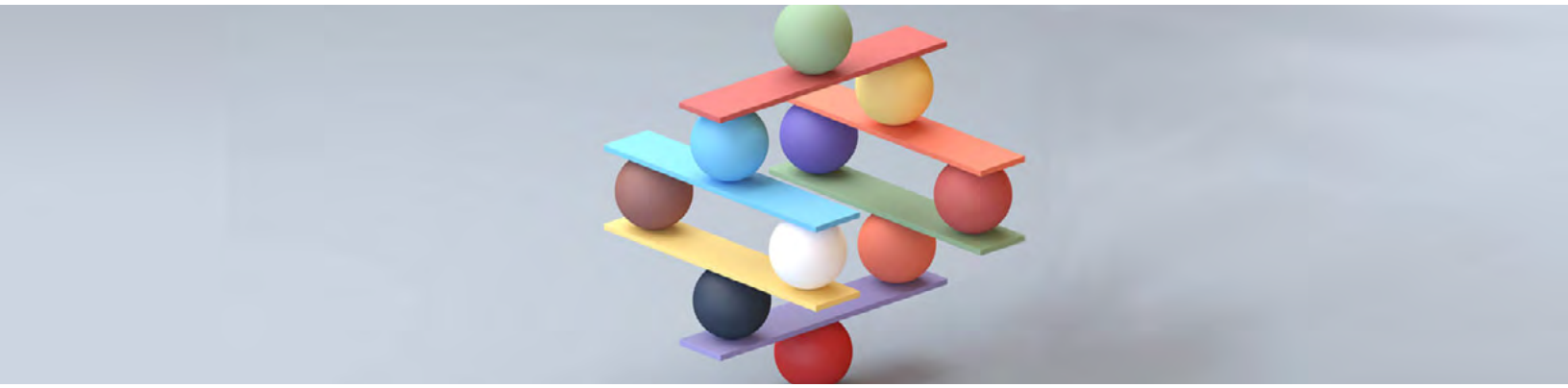
Unfortunately, there isn't a cookie-cutter approach because no two sites are exactly the same, but with understanding of the fundamentals used for planning, the estimation of these costs becomes more accurate and effective.

ANDREW BUGEJA IS AN ELECTRONIC SECURITY PROFESSIONAL FROM MELBOURNE, AUSTRALIA. BUGEJA HAS MORE THAN 15 YEARS OF EXPERIENCE IN THE SECURITY INDUSTRY. HE SPECIALIZES IN ELECTRONIC SECURITY DESIGN, MAINTENANCE AND UPGRADE WORKS TO PREDOMINANTLY BROWNFIELD SITES. WHILE WORKING FOR INDUSTRY LEADING ELECTRONIC SECURITY PROVIDERS, BUGEJA HAS WORKED WITHIN A VARIETY OF SECTORS DELIVERING INNOVATIVE SOLUTIONS TO DEFENCE, CORRECTIONS, COMMERCIAL, AND RETAIL CLIENTS. BUGEJA HOLDS A DIPLOMA OF BUSINESS FROM SWINBURNE UNIVERSITY OF TECHNOLOGY AS WELL AS A TRADE QUALIFICATION IN ELECTRONIC SECURITY FROM BOX HILL INSTITUTE.

Balancing Needs and Wants Against Situational Realities in Campus Security

As the threat landscape has changed, security leaders have had to adapt. It is infinitely important that the leaders responsible for the safety and security on university and healthcare campuses comprehend and strike a balance between needs versus wants as they build their programs to respond to changes.

By Lisa Terry, CPP



As the threat landscape has changed, security leaders have had to adapt. It is infinitely important that the leaders responsible for the safety and security on university and healthcare campuses comprehend and strike a balance between needs versus wants as they build their programs to respond to changes.

In this Q&A series, four tenured campus security leaders share how they address building and fortifying their programs amid change.

CONTRIBUTORS:

Frank Spano serves as director of education security services at Allied Universal, the largest provider of security services to colleges, universities, and K-12 institutions in North America.

John H. Dailey is chief of police for Duke University in Durham, North Carolina, where he oversees a staff of more

than 180 people dedicated to serving the Duke community.

Bonnie Michelman, CPP, CHPA, serves as the executive director of police, security, and outside services at Massachusetts General Hospital and Mass General Brigham, a 17-hospital, 90,000-employee organization.

Lisa Terry, CPP, CHPA, serves as the vice president, healthcare, for Allied Universal. Prior to that she served as director of hospital police and transportation at the University of North Carolina in Chapel Hill.

WHERE TO START

As with many aspects of life, often the most difficult step is getting started. Understanding this somewhat inherent challenge is the first step toward positive progress. In this section, explore the essential components of getting started: determining overarching goals, identifying and empowering individuals and organizations, quantifying quality and effectiveness, and emergency and contingency planning.

How do you determine your program's overarching goals?

Frank Spano. To be truly effective, program goals must interface and complement both the larger organizational goals and the campus community's intent. Program goals must embrace the spirit of the larger organizational goal while adjusting as needed to address specific challenges and opportunities applicable to the specific program's needs and desired outcomes. Similarly, the program goals have to be in tune with the campus community's intent.

More and more, campuses are adapting to identify, codify, and embrace the overall perceptions, desires, and beliefs that form the community's identity, norms, and brand. Though not the primary driving force when com-

pared to overall organizational goals, campus community intent is increasingly relevant and applicable in shaping programmatic goals and procedures.

John Dailey. It is important to constantly monitor the landscape—nationally, locally, and institutionally—to determine shifts in expectations thus shifts in goals. Quality and effectiveness of our programs may need to be balanced between community expectations and what we know is the right thing to do.

Bonnie Michelman. Through our strategic plan which we update every three years and through the organization's goals each year. We review the mission and strategic goals and areas of focus for the hospital in general. We look at changing trends, vulnerabilities, and where are attention is most needed. Goals also must be nimble and able to change if major issues strike and resources and focus must adjust.

Lisa Terry. It is important that we develop or assist in the development of the hospital's security strategic master plan, which essentially lays out the security philosophies, risk, mitigation, preparedness strategies, and overall goals. The security master plan is usually written for a three-year cycle with annual updates.

Who should be involved?

Spano. Campus communities are best positioned to establish and advance organizational and programmatic goals through cross-functional teams composed of representatives from across the institution's various departments, constituencies, and thought groups. This is often easier said than done because senior leaders within and outside the campus community are reluctant to fully embrace leadership by committee—and for fairly good reason. That said, every effort should be made to cast a wide proverbial

net to engage as many aspects of the campus community as possible.

Michelman. I think it is most important for the senior security leadership team to be involved and determine a plan that uses others in the department for feedback, senior leadership for macro decisions, and often most important, other partner departments with which you have complementary and supplementary relationships. This can include the emergency department (ED), nursing, emergency preparedness, human resources, psychiatry, and other support services. Getting buy-in and ensuring others agree with your goals and priorities (or at least understand them) are critical to being successful.

Terry. The security master plan should be developed by the security department senior leaders in concert with hospital administration and supported by the organization's overall strategic plan. It is important that input is solicited from emergency management, risk management, and leaders from other security sensitive areas.

How do you define quality and effectiveness of a program? Can it be quantified?

Spano. While quality can often be quite subjective—I prefer this hamburger over that hamburger, etc.—effectiveness tends to lend itself to a greater degree of objectivity. Campus communities are asked to quantify both the subjective quality and more objective effectiveness of all manner of programs—from graduation rates and satisfactory academic progress to organizational accreditation and reportable crimes and events. At the end of the day, quantification is often some combination of disclosures pursuant to regulatory and accreditation requirements, internal benchmarking against pre-established key performance indicators (KPIs), external benchmarking against known best prac-

tices and contemporary standards, and feedback from end users within—and related to—the campus community.

Michelman. There are some metrics that can help define the effectiveness of a program and quality standards. These may include numbers and trends of incidents, lost work time, injuries, and legal action, but this doesn't tell the entire story. Your staff turnover is an important way to measure quality, with trends going down or changing (incidents may be higher, but it could be that people are trained better to report things they didn't before—which is a good thing). The quality of security staff, the depth and trust of partnerships within the organization, and the relationships with relevant agencies outside the organization all impact the quality and effectiveness of your program.

Doing deep dives into data analysis to uncover trends and then redeploy resources is critical. How you manage a serious event also can be a great measure of effectiveness. Good communication strategies are essential.

Terry. The healthcare industry associates quality and effectiveness with outcomes, especially patient outcomes. It is extremely important that healthcare security practitioners measure the effectiveness of their programs by their impact on various outcomes as well. For instance, measure and reduce the number of injuries via patient assaults on officers over time due to additional training and PPE (bite sleeves, face guards) or measure and reduce the number of assaults or worker's compensation claims to clinical staff over time due to additional training, etc. The amount spent on training and equipment can be quantified and compared with the amount spent on worker's comp, turnover, recruitment, etc.

How do you plan for emergencies and contingencies that could impact program goals, quality, and effectiveness?

Spano. Today's environment has reinforced the notion

that the impossible is at least probable. For example, had you asked me a year ago if I believed a shirtless man in a horned fur hat and his compatriots would make their way past countless protective layers into one of the centers of American government, I would have told you that you're crazy. But, today, this doesn't seem too far outside the scope of possibility. The same applies to the myriad threats facing today's campus communities.

Organizations are increasingly being tasked with identifying the unknown, making sense of an ever-convoluted mass of competing information, and identifying the needle in the haystack that is most likely to do harm. Thankfully, developing technologies, third-party assessments, external benchmarking, and good old-fashioned community engagement strategies are continuing to develop as a reliable solution suite to an ever-complicated problem set.

Michelman. Planning can be done through emergency preparedness training of different types done frequently—tabletop and functional drills. We start with an all-hazard approach, take great time with a large multidisciplinary group to do the hazard vulnerability assessment, and try to cue off of that. We use situations occurring at other hospitals and other organizations, liability information, and then benchmark for excellent practices and new methodologies that can help. Our Hospital Incident Command System (HICS) command structure helps a great deal as does our relationships with outside agencies to join us in our planning or guide us. We have learned a lot about the need for longitudinal planning, for getting all staff involved in planning and preparation, and in realizing that time spent in contingency planning is time well spent.

Terry. As security leaders, it is important that we develop or assist in the development of the all-hazards hospital emergency operations plan as it pertains to security and

emergency staffing. An all-hazards approach is an integrated method to emergency preparedness planning that focuses on capacities and capabilities that are critical to preparedness for a full spectrum of emergencies or disasters both internal and external. Because the HICS was created for use in both emergency and non-emergency situations, I have it to be an excellent resource in building the plan.

It is also important to review the organization hazard vulnerability analysis so that you can pre-identify various security functions associated with the threat levels of the respective disasters. In fact, the scope and scale of work for security may change significantly based on the emergency.

As the duties associated with the job change and additional security staff must be added, your plan should reflect how you intend to meet those staffing demands. "Just-in-time" training for additional staff and for additional job functions should be considered.

GATHERING DATA

Why do we need to collect data, and what data do we need?

Frank Spano: Is there such a thing as too much data? Perhaps. Though one might argue the critical distinction is that of data versus intelligence. The former being raw information, while the latter is information refined through analysis and application into something of particular value to the organization. In a world of seemingly never-ending data, our challenge lies in the effective consolidation, analysis, and interpretation of that raw information into something of value to the campus community. As mentioned previously, campuses collect all manner of data, and often employ individuals or entire divisions to do institutional research. Thankfully, the somewhat natural inquisitiveness inherent in academia

provides a significant leg up when it comes to data collection and analysis.

But what's actually important? It depends on the organizational goal to be measured. For some applications, such as regulatory or accreditation reporting, event data and raw statistics are satisfactory. In other cases, such as the evaluation of key performance indicators (KPIs) related to organizational or programmatic goals, raw statistical data would prove insufficient absent additional analysis and application to the specific situation relevant to participation, application, and outcome.

John Dailey: We need data to make a real impact on the problem. Through analysis, we can develop targeted approaches. For example, reducing workplace violence is an imperative goal in healthcare. A targeted strategy might be to understand and reduce the number of times patients hit staff—this requires data.

Lisa Terry: Collecting and analyzing appropriate data is an essential piece in building and expanding a quality healthcare security program.

To better pinpoint the key pressures or drivers relating to security incidents, it is important that the data collected be relevant and current. In building the data set from which to collect the information (compare and analyze over time), there are three areas to be considered. It is also advantageous if you are able to compare multiple facilities at once. I took recommendations from an article written by Katherine Eyestone and Shon Agard, MS, CHPA, in the *Journal of Protection Management* in titling the data set:

1. **Risk Characteristics** (community crime rate, CAP Index, ED visits, etc.). These are characteristics that affect security but over which the security leader has no control.

2. **Security Program Characteristics** (hours per week, de-escalation/non-escalation training, visible video surveillance, visible emergency communication system in parking areas, equipment/PPE,). These are characteristics that affect security which the security leader has control of.
3. **Outcomes** (Worker's compensation claims, assaults including hits, kicks, bites, spitting, and threats, etc.). Measurements of impact over time.

A simple spreadsheet, similar to the example below, allows you to document the chosen risk characteristics, the security program characteristics, and the outcomes from each healthcare facility for which you are responsible. Once you have a snapshot of your entire system, you are better prepared to review your security program over time and perhaps make changes as necessary to affect the outcomes.

Where can we get the data within our organization and outside our organization?

Spano: Perhaps the most consistently recurring conversation I have with campus leaders revolves around the all-too-real notion of campus communities being divided into various silos: academic, athletic, administrative, etc. Though I'd like to tell you this only exists in enormous academic institutions with large standalone schools and programs, it seems to be the case even in the most seemingly tightknit small-footprint institutions.

Unfortunately, this has a tendency to lead to difficulty in capturing accurate data—or data at all—from across various silos. Often, information is withheld or otherwise massaged so as to cast the respective silo in the best light prior to submission. Unfortunately, this poisons the data set and artificially skews results. For this reason, campus communities

are well served in identifying and empowering a cross-functional team led and supported by external facilitators to collaborate across silos to create an environment conducive to obtaining the most relevant and un-edited data for analysis and application.

Bonnie Michelman: From an internal perspective, data can be obtained through incident reports, quality and safety reports, occupational health reports, and other mechanisms set up to capture whatever activity and data within the organization.

Outside agencies and companies can provide great supplementary and complimentary data as well. Having a report done of the crime risk at facilities you own or lease offers you a clearer picture on what type of security you need. Getting data and/or trends from regulatory or accreditation agencies and using professional organizations like the International Association of Healthcare Security and Safety (IAHSS) or ASIS International can offer guidance, standards, and great data, such as the *IAHSS Foundation's Annual Crime Survey.*

Collecting information on negligent and inadequate security litigation across the country can help you ensure you are avoiding the prevalent risks and utilizing reasonable standards and practices in your operation.

Finally, benchmarking with other colleagues in your industry and others can offer great insight and data to help you formulate plans and make decision.

Terry: In addition to internal department incident reports, organization risk, and quality and safety reports, comparative data may be obtained from the ED or behavioral health unit on number of visits, as well as the finance department, on the number of adjusted discharges. External data may be obtained from the U.S. Department of Labor's annual reports on occupational injuries, illnesses, and fa-

talities based on the industry. Other associations such as the American Hospital Association (AHA) and IAHSS release regular studies on violence in healthcare.

How can we interpret the data we get? What does it mean? How does it affect what we want?

Spano: As there is a broad range of data sets applicable to campus communities, so too is the wide spectrum of interpretation methods. While largely driven by outcome requirements—such as annual security reporting (ASR) accreditation, and reaccreditation evaluations—data interpretation can range from simple reporting to more complex analysis involving end-user feedback surveys, data compilation and assessment, and increasingly electronic statistical analysis.

Dailey: An example of our use of data can be found in our response to propped door alarms throughout campus. A significant number of doors throughout the university are controlled by electronic access control. In 2017, we had more than 28,000 propped door alarms. That's an extremely high number. Each of these alarms required a security response and report back as to status. Many times, the door was secure by the time the response occurred.

Though we had hoped to find a pre-existing proven plan elsewhere that could work, we ended up having to build our response from scratch. We established a cross-functional team consisting of public safety and university information technology personnel to look at the data, the time at which each alarm occurred, the length of time each propped door was unsecured, the acceptable time threshold for each propped door, and the response time to get there.

From there, the team drilled down into the data set, divided the doors into various levels of priority, and made recommendations on how best to structure response operations for each priority level.

For example, the door to a classroom within a building may be a lower priority—particularly after business hours—than the door to a residence hall where people live or congregate on a more 24/7 basis. This data-driven process allowed us to balance security needs against operational needs, and resulted in a drastically reduced call volume down to approximately 19,000 propped door alarms the following year.

The team continues to provide data assessment and analysis year-over-year to ensure we are responding effectively.

The cross-functional team allowed us to reprioritize an unsustainable issue, identify reasonable solutions, and implement meaningful response.

Michelman: The department should have people who are trained on data collection, analysis, and trends. Some have an intelligence resource within the department or the investigative function. Reports that are data based need to be compiled monthly and yearly to show trends to help with investment of security equipment, staff, and technology, along with resource deployment.

Plans and strategies need to be continually adjusted based on data analysis and trends being seen. If there is more violence in the ED on weekends or a particular shift during the week, operational changes should be made. If intrusion or piggybacking is happening on particular doors or areas, better surveillance and training of those in the area has to occur.

It is important to discern nuances such as higher reporting due to increased training, which could skew actual incidents and risk. Your security staff needs to be able to capture very thoroughly in incident reports any specific factors that point to causation or a change. This is critical for planning.

Terry: As an example of how data can be analyzed, in the chart below Hospital B continues toward the goal of a

restraint-free environment, the number at the bottom of the graph remains at a constant flat line. However, approximately 50 percent of the "Total Security Calls for Service" involve some type of physical management or intervention for patients by security. Fewer patients are being physically restrained. However, there are still a high number of physical management situations in which the security department is involved due to a high level of clinical aggression. This data analysis allows us to determine the importance of ongoing monitoring of this type of activity to ensure that adequate training and staffing are being conducted for the security officers.

It is very important to compare data over time, to include years. For example, the initial hypothesis at Trauma Hospital A was that with more patients being seen in the ED, there would be more weapons collected at the magnetometer. However, as shown in the graph below, the numbers showed a substantial decrease in weapons collected each year. Upon further examination, it was determined that many of the individuals who visited this ED had visited it in the past (more than once). These individuals liberally shared the fact that the ED was equipped with a standalone magnetometer, deterring individuals from entering with a weapon.

What can we do when the different data sets don't agree?

Spano: My college statistics professor once told our class that the best thing about statistics is that with the right calculations, the data outcome can be whatever we want it to be. If this is true—and experience tends to indicate it may be at least partially—then campus community leaders have a twofold obligation as to data analysis and interpretation.

First, an obligation to the data itself in taking all necessary precautions to safeguard the validity and accuracy of the outcome rather than falling into the trap of data manipulation. Second, an obligation to trust the data process insofar as doing so will provide the most accurate—if not always rose-colored—data to frame program assessment and future planning. If we adhere to these two obligations within a collaborative environment, data set disagreement should be greatly mitigated. That said, in the event disagreement persists, it may be necessary to enlist the support of a third-party in providing investigation, collection, and analysis support to identify the most accurate data set and outcome picture available.

Michelman: If data sets do not correlate, a deeper dive into the data with others needs to occur. Determine common definitions and good training on ways to submit data then ensure a constant crosswalk with other data sources is being done to determine consistency and accuracy. Often issues that complicate this are a difference in definition of incident or event, or ambiguity about when or who to report something to. It may require changes to your software program to ensure consistency and reliability of data.

Terry: I recommend that regular audits are conducted for all of sources of data to maintain its legitimacy and accuracy. If the data is being compiled within the security department, it is important that objective, specific written procedures are followed in obtaining and analyzing the data.

USING DATA

After we get the data, how can we determine what we want to happen? What actions do we need to take?

Frank Spano: When compared with refined intelligence, raw data can often be overwhelming. Upon collection, data should be analyzed, confirmed, and applied in a way

that advances the particular requirement. For example, simple statistical data that might satisfy reporting requirements under the Clery Act may prove insufficient for more complex evaluation such as internal institutional research or external accreditation review. As a result, one of the critical aspects of statistical data management is to have a solid understanding of the intended goal the data seeks to advance or support.

John Dailey: Once we have the data, sharing across the organization is important for transparency and solutions. Data is a living thing, and the mission or data creep begins when you don't stay on top of it.

Not all data is created or used equally. For example, when compared to propped door alarms which are unique situational occurrences, data collected from card access—which is used for everything from access control to dining services and other on-campus purchases—provides fewer tangible data sets from a security perspective but much more relevant data sets from an operational perspective. Such information is usually tied to a specific individual and can be used for forensic or investigatory efforts, but they have limited applicability in identifying and responding to an immediate threat when compared to, say, a propped door alarm.

Bonnie Michelman: Analysis by the management team needs to be extensive to determine what services need to be augmented or eliminated, where resources many need to be moved, where additional training may be important in the organization and what security technology needs modification or enhancement. Procedures and policies may need to be created or adjusted based on data.

It is critical to share the data and its implications with the entire security staff (which often doesn't happen) along with relevant departments so they can help be part

of the solution. The danger is getting data that should drive a change or a new procedure and then not doing anything once the risk is known. Having routine meetings with a multidisciplinary group of colleagues to review the data and discuss modifications to operations makes this a formal and consistent expectation for everyone.

Lisa Terry: Developing a risk stratification model similar to the example that I have shared below (and based on a similar model from Katherine Eyestone and Shon Agard, MS, CHPA in the *Journal of Protection Management*) is very helpful is organizing and displaying the data and follow-up actions.

The green, yellow, and red colors are risk heat map colors based on CAP index scores. The HPW are the hours per week that security officers are physically on site at that location. The additional risk factors at each location include outpatient behavioral health unit located on-site; high adjusted discharges (high number of outpatient services); lack of exterior lighting; emergency department (ED); inpatient behavioral health unit; and off-campus parking for staff or patients. Reported assaults are important to note. Officer tenure can be important if turnover is high and appropriate training is not occurring. Mitigation and follow-up actions may then be deployed (and displayed), as necessary.

How can we balance the data we get with our experience, gut feelings, and organization mind-sets or opinions? How can we find middle ground?

Spano: Perhaps thankfully, technology still isn't at the level where it can replace the inherent gut feeling that comes from decades of personal and professional experience interacting within and outside the campus community environment.

In everything from data analytics to on-ground community engagement and customer service, there is little doubt as to the continuing value of human interaction and experience as a critical component of tactical, operational, and strategic decision-making and application.

That said, there is a time for reliance on the gut feeling and a time for reliance on the data. Oftentimes, this is a combination of the two, and it provides an excellent platform to present and consider a series of potential solutions or outcomes. Trust your instincts, but verify through data.

Dailey: Data isn't always going to match up perfectly. But when it doesn't, we rely on subject matter expertise and professional opinions to guide the institution toward the truth.

Case in point, when we encounter potential data points that may not add up when reviewing Clery Act data, we rely on individuals who have advanced specific knowledge and training—to include our general counsel—to identify the proper course of action. We reinforce this through face-to-face meetings to review each and every potential Clery Act reportable.

The data is the data. What the institution is looking at us for is to anticipate next issues—issues created or enhanced by national or local events, as well as those arising within the campus community itself. In the security and law enforcement community, anticipating what's next is somewhere between the gut feeling and our personal and professional experiences, which help guide our anticipatory actions. That said, we have to be careful not to adhere solely to those gut feelings at the detriment of paying attention to the information and intelligence we're receiving. The data may lead us a different way, and we have to be open to that.

Michelman: Getting experiences and feelings from a credible number of multidisciplinary employees (and

even patients) may help to navigate this balance with metrics and data that has been obtained. Surveys and risk assessments also help with this.

I think this question is important because data is a tool but not a perfect science. Getting the feelings and feedback from many may offer trends that are accurate and that data doesn't achieve. Asking lots of questions of your security staff, frequently, and meeting with nurses, physicians, and those from other role groups to understand the climate and concerns will go a long way. This is also important for abating incorrect information that has become publicized or discussed and share accurate activity and response instead.

BUILDING CROSS-FUNCTIONAL TEAMS

Why develop these teams in the first place?

Frank Spano: Campus communities are often plagued by a silo mentality wherein individual departments, schools, programs, or even individuals share data within tightly controlled vertical channels or silos rather than across the wider horizontal community—often at the detriment of constituents such as students who tend to exist outside the more formalized organizational structures.

John Dailey: Having the input and buy-in from multiple departments and multiple levels is critical to sustained success. Clinical, legal, compliance, administration, safety, and security all have a role. Teams are important—campus security and law enforcement are evolving from looking at things through a somewhat closed "this or that" perspective to incorporating more diverse and often differing perspectives unique to the campus community in order to create truly meaningful solutions or public safety.

Bonnie Michelman: It takes a true village to mitigate risk and diminish violence and other issues in the healthcare arena.

Healthcare vulnerabilities are diverse, and there are many often changing quickly. Having others from many departments can expand your ability to have trained and aware people who assist with the protection and risk management efforts.

Security cannot be effective without mutual trust and understanding with all constituents, without good team building and bonding within themselves, and without understanding the mission and goals for the department. Everyone working in a healthcare facility needs to have an understanding of security, its importance, and how to use the services of the security department. People need to clearly know the breadth, depth, and expertise of the security team and how they can help with protection of the organization.

Generally, hospital employees and certainly security staff need to be empowered to make a difference, to diminish risk and to share concerns. If the security team is not included in important strategic discussions, it cannot maximize its effectiveness. It needs to be a full part of the healthcare team and feel that involvement and respect while also reciprocating it.

Lisa Terry: The 2017 McKinsey & Company comprehensive study of more than 70,000 employees from more than 200 companies did a great job in answering the question of why we should build cross-functional teams. The top-performing companies in the group they surveyed had the highest ratings in these measures:

- A diverse workforce promotes creativity;
- Challenging opinions on operational requirements defies the status quo because constantly defying the status quo is how organizations evolve; and
- A diverse mix of voices leads to more robust discussions and better outcomes.

Please provide examples of potential partnerships (internal and external). What are the synergies among these various stakeholders?

Spano: One of the critical elements of truly effective cross-functional teams is external involvement from trusted advisors, professional organizations, and related service providers. This ensures the most equitable and targeted facilitation of efforts, and it maximizes the opportunity for external benchmarking throughout the data collection, analysis, and implementation phases of effort. We find that our role in facilitating cross-functional groups provides additional opportunities to break down institutional silos, leverage best practices, and encourage an open and accountable data-driven organization.

Dailey: Of course, a large part of campus safety and security data revolves around the Clery Act. To ensure we have the most comprehensive data set to meet the regulatory requirements, we established a Clery compliance committee. This is an institution-wide organization, chaired by our vice president for administration, and it brings together representatives from all key components, athletics, general counsel, student life, human resources, Title IX, diversity and inclusion, and the like to report and collect data in one central function. This helps keep everyone on the same page and works to break down institutional silos.

The keys to establishing genuinely cross-functional teams capable of horizontal operation across a series of vertical institutional silos are twofold. First, it is critical to have the appropriate level of senior leadership emphasis and support. For example, our Clery committee shows institutional commitment and encourages involvement.

Second is relationships. Sure, there are regulatory compliance requirements that bring us together, but it's about

building and developing relationships and people being able to work together. As campus security and law enforcement professionals, we work every day with different institutional organizations with different priorities and responsibilities, and continuously work to build trust in their minds that we're going to do the right thing when it comes to the information we receive.

Terry: There are numerous partnerships among various stakeholders. One example that stands out in the healthcare arena is the synergy derived between a safe and secure clinical environment and that of a productive workforce and gratified patient population. To establish this synergy, several internal and external partnerships must exist. These partnerships include security, patient safety, nursing, compliance, risk management, human resources, as well as external regulatory agencies.

Should we reach out to peers at other organizations or campuses?

Spano: There is tremendous value in benchmarking against other campuses. While each campus community is unique, there are far more similarities to be found across various campuses than there are differences.

Dailey: Yes. Our job is to serve our community—not to do things to the community. Where there may have been more trust that we're doing it as they like, there's much more interest today in how we do that. The best way to do that, and how the campus community interprets what we provide, are purpose-built feedback groups and programs.

Michelman: Absolutely. Hearing other professionals' issues, mistakes, successes, and best practices while sharing yours helps everyone to improve their ability to be successful. This is critical to having an enlightened and successful security program.

We learn and grow together in this complicated arena and sharing your successes, mistakes, not having to always reinvent the wheel and simply having people you can collaborate or share with is invaluable. Community takes on a larger meaning as we all try to navigate changing risks, foreseeable and unforeseeable events, and the emotional and sometimes dangerous milieu of a healthcare facility.

Terry: With appropriate approval, do not hesitate to reach out to colleagues with whom you have built a relationship of trust and who may have previously led a change in his or her organization. Be willing to for ask assistance. You may be pleasantly surprised at what you discover.

Who's Liable for an Active Shooter Incident? Expectations Are Changing

As mass shootings continue to rise in the United States, courts and the public are shifting their perception on who is ultimately responsible for protecting potential victims.

By Megan Gates

A gunman opened fire on a McDonald's in San Ysidro, California, in 1984, killing 21 people and injuring 19 others. The incident was one of the first modern mass shootings to be followed by a negligent security lawsuit. Victims' families and survivors sued McDonald's, arguing that the company was negligent because it did not hire private security for the restaurant despite its location in a high crime area. The court disagreed.

The "deranged and motiveless attack...is so unlikely to occur within the setting of modern life that a reasonably prudent business enterprise would not consider its occurrence in attempting to satisfy its general obligation to protect business invitees from reasonably foreseeable criminal conduct," the Court of Appeals of California wrote in its decision (Lopez v. McDonald's Corp), dismissing the case.

Today, however, mass shootings in the United States are not rare events. As of Security Technology's press time, there had been 371 mass shootings—incidents where four

or more people, not including the shooter, were killed or injured—in the first seven months of 2022 alone, up from 272 total in 2014, according to the Gun Violence Archive.

The increasing number of these incidents is having an impact on how courts assess liability when a shooting occurs because mass shootings are no longer as rare as a "meteorite falling" from the sky, says Michael Haggard, managing partner at the Haggard Law Firm, who is representing the families of two victims and a teacher injured in the 2018 Parkland high school shooting.

"Liability for businesses in mass shootings is something they should be very, very concerned about," he adds. "Every business, every school better have a security plan to deal with mass shootings. And they better enact it because if they don't, they are going to be found liable."

A Shifting Landscape

How courts assess liability changes over time in response to precedent, new laws, and societal evolution. After attending a conference where the issue of liability in response to mass shootings was raised, Michael Steinlage, partner at Larson King, decided to dive into the topic.

His research resulted in "Liability for Mass Shootings: Are We at a Turning Point?" published by the American Bar Association in February 2020, which identified that before the 1966 University of Texas shooting, there were only 25 public mass shootings where four or more people were killed.

"Since then, the number of such shootings has risen dramatically, and many of the deadliest shootings have occurred within the past few years," Steinlage wrote. "Of the 220 incidents that occurred from 2000 to 2016, nearly half (107) took place in an education, retail, or government/military setting."

Additional insights from Haggard's firm based on re-

search from Harvard University and Northeastern University found that mass shootings are increasing. Since 2011, for instance, mass shootings are occurring every 64 days in the United States—up from an average of every 200 days prior to 2011. And six in 10 Americans are now concerned that a mass shooting could happen in their neighborhood.

Steinlage's analysis looked at third-party liability for mass shootings—where an individual sues a business or another entity for causing alleged harm. He particularly focused on how, in most instances, business owners are not considered liable to individuals who are injured by the criminal acts of another person unless that act was foreseeable—such as the business receiving a specific threat in advance of an act of violence. Courts have also upheld that "foreseeability of mass shootings cannot be established through local crime rates or general evidence of a criminally active environment," Steinlage wrote.

Since February 2020, Steinlage tells *Security Technology* that more companies are being sued for having some role in failing to stop or failing to identify a shooter before an incident. It has also become more difficult for those lawsuits to be dismissed in the early stages of the suit, given how the law has developed about the role companies should take in preventing these incidents and around the subject of immunity.

"It comes down to the scope of their duty, which is generally measured by the concept of foreseeability and is something a risk? Is it something foreseeable that they knew something about? And should therefore have a duty to do something to prevent it?" Steinlage says. "Traditionally, the courts said nobody could foresee or be responsible for random acts of violence from a third party. Over the years, courts have started to chip away at that and held that in some cases, these types of events might be foreseeable and

there is some duty to take precautions against them."

One recent case that struck away at this concept was *Wagner v. Planned Parenthood Federation of America, Inc.* In 2015, a gunman had traveled with weapons to the Planned Parenthood clinic in Colorado Springs to wage "war" because the clinic provided abortion services, the U.S. Department of Justice said. The attack killed three people, including a police officer, and wounded eight others.

The plaintiffs in the lawsuit argued that if the Planned Parenthood clinic had taken certain security measures, the gunman might not have been able to gain access to the building because he encountered more resistance—and could have been stopped before carrying out further violence, Steinlage adds.

The Planned Parenthood case was initially dismissed due to lack of foreseeability. On appeal, though, a higher court reversed the dismissal, and the Colorado Supreme Court upheld that decision to let the case proceed to a jury trial. In October 2021, a jury ultimately decided that Planned Parenthood was not liable.

To avoid this in the future, Colorado Governor Jared Polis in April 2022 signed into law legislation that clarifies landowner liability based on the Colorado Supreme Court's ruling. The Colorado law now says that foreseeability for third-party criminal conduct cannot be based upon whether the goods or services provided by a landowner are controversial.

Another major series of cases closely watched to assess how liability is shifting were civil lawsuits filed by the families of victims of the Virginia Tech University shooting. The attack was carried out by a student and resulted in 32 people being killed and 17 being injured. Initially, a jury ruled that the university was liable for the deaths of Julie Pryde and Erin Peterson.

Later, however, the Virginia Supreme Court overturned that decision because the university did not have a duty to warn students about the potential for criminal acts being carried out by a third party—in this instance, a fellow student.

SETTLEMENTS OF NOTE

Some recent mass shootings have led to major settlements on behalf of property owners and their insurance providers with survivors and victims' families, such as the $800 million settlement from MGM to victims of a shooting targeting a Las Vegas music festival carried out by a gunman staying at an MGM property. But that does not mean that a jury would rule in victims' favor in every case that went to trial, Steinlage adds.

For instance, juries might still be inclined to say the shooter is the true cause of damage and that a business could not always be expected to know it was a target.

"There is an argument that it's just not fair to expect that a business should protect itself against a random person intent on violence," Steinlage says. "Given how many guns there are in the United States, it's an impossible task. I haven't seen a court use that as grounds for granting or denying summary judgement on a legal basis, but you could see a jury doing that."

Other tactics on changing the way liability is assessed are also in play.

Since 2005, firearm manufacturers have been shielded from liability from crimes carried out using their products under the U.S. Protection of Lawful Commerce in Arms Act. But after the Sandy Hook Elementary School shooting in December 2012, families of nine victims sued Remington—the manufacturer of the firearm used in the shooting—with claims that its product should never have been

sold to the public. The case reached the Connecticut Supreme Court, which ruled that under state law the families could sue Remington for how it marketed its firearms.

Remington appealed the court's decision to the U.S. Supreme Court, which declined to take the case. The company then agreed to a $73 million settlement with the families in February 2022, according to the Associated Press. The settlement amount is covered by insurance companies that represented Remington, which also filed for bankruptcy.

The settlement marked some recognition of the potential for liability, Steinlage says, adding that the same could be said for the MGM settlement. MGM was "fortunate" that it had a "significant amount of coverage that was able to pay out on the claim," he explains. "But they wouldn't have paid out if they didn't think there was a real risk of liability."

Since the announcement of the Remington settlement in February, the U.S. state of California has passed legislation—effective in 2023—that will allow state, local government, and Californians to sue gun manufacturers for the harm their products cause.

While the California law does not directly address school and campus security, Haggard says it represents a "huge advancement" for the ability to hold gun manufactures liable for mass shootings and mass shooting negligence.

"Now these cases are going to trial, so it's an issue for every business," he adds.

THE INSURANCE IMPACT

With the changes in court proceedings and U.S. state laws, insurance providers may be requiring organizations to take additional steps to mitigate the threat of a mass shooting or might provide resources to implement those steps.

Marsh McLennan—a global insurance provider—underwrites active assailant coverage, also known as active shooter coverage or deadly weapons coverage, that also typically covers the costs of advisory services to help businesses assess their risk, conduct training for employees, and develop active shooter response plans.

Additionally, the policies typically cover property damage, business interruption, legal liability, non-physical damage, loss of attraction, reimbursement for consultant services and post-incident care, and additional security.

"Some of the earlier policies provided for enhanced security on the anniversary of an event on the assumption that in some cases, there's a greater likelihood of something occurring," Steinlage says.

But with the number of shootings on the rise in the United States, Steinlage says that policies may become more expensive. Analysis from the *Insurance Journal* found that costs for insurance protection from mass shootings rose more than 10 percent in the United States in 2022, with clients looking to purchase policies to cover $5 to $10 million compared to $1 to $3 million in 2018.

Steinlage also added that these policies may include more exclusions for the types of incidents that can be covered.

"There are already assault and battery, and firearms exclusions in bars and restaurants," Steinlage says. "More and more of those types of exclusions are showing up in a broader range of policies."

POLICY AND TECHNOLOGY

U.S. lawmakers are also changing their approach to firearms. In June 2022, U.S. President Joe Biden signed into law legislation that expands background checks for potential firearms purchasers under age 21, invests millions of dollars into intervention programs for mental health,

tightens restrictions on trafficking guns and making straw purchases, and creates additional resources for local governments to implement red flag laws—which allow authorities to temporarily confiscate firearms from individuals determined by a judge to be too dangers to possess them.

The new law, however, does not make major changes to the number of firearms already in circulation in the United States, which means that security teams will continue to play a large role in preventing and responding to shootings.

Insurance providers may be requiring organizations to take additional steps to mitigate the threat of a mass shooting or might provide resources to implement those steps.

With the school shootings at Columbine, Sandy Hook, Parkland, and Uvalde, Haggard says that every school district should be looking at access control measures to protect their campuses.

"When you think of Sandy Hook, Uvalde, and Parkland, all three of those shooters came from off-campus. None of them were students who snuck guns in," Haggard explains, adding that schools need to take a look at how people are gaining access to their campus, and the type of security that needs to be implemented to harden their access control.

Additionally, security measures should be in place to control access and screen visitors for events on campus—such as metal detection wands or bag searches at football games or musical performances.

Haggard also suggests campuses look to adopt technology that can automatically detect when a gun has been fired to initiate an immediate lock down and response.

"There's technology out there that the minute there's a shot, they can identify what type of weapon it is, notify the police, and more importantly, shut down the school," Haggard says. "An alarm goes off, every teacher pulls their doors—reinforced doors—and every classroom is shut down. There's no way anybody's getting in there."

One security measure that has been enacted in some areas—allowing teachers to carry firearms on campus—is not one Haggard recommends, however, saying it is not a solution to address an active shooter armed with an AK-47 or AR-15.

"If the federal government does not want to take away these weapons of military advancement, then target harden the schools," Haggard says. "Access control, security out front, and other technology inside the school. That's not chump change, but if we're not going to get rid of the guns, we better do something."

MEGAN GATES IS EDITOR-IN-CHIEF OF SECURITY TECHNOLOGY. CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

SECURITY MANAGEMENT

Behind the Façade: Negligent Security and Premises Liability

Jurors expect landlords and property management companies to exercise a reasonable standard of care in protecting tenants from violent crime. The law demands it.

By Steven C. Millwee, CPP

The Georgia Court of Appeals upheld a nearly $43 million verdict against a CVS Pharmacy in southwest Atlanta over a parking lot shooting during a robbery that left a man with permanent serious injuries. Defense attorneys raised several objections to the verdict. They argued that the victim was just as much to blame as CVS and that the jury verdict should be voided since they did not lay any blame on the unknown shooter. The court disagreed. (Georgia CVS Pharmacy, LLC v. Carmichael, Georgia Court of Appeals, 2021)

Plaintiff James Carmichael arranged to meet a man in the parking lot of the CVS to sell an iPad in 2012. After exiting his vehicle, the shooter appeared and put a gun to Carmichael's head, demanding money. Carmichael complied, then grabbed his own gun and attempted to fire. Instead, the robber shot Carmichael several times in the stomach and back, leaving him with permanent nerve damage after multiple surgeries.

Carmichael sued CVS for premises liability, and in 2019 a Fulton County jury returned a verdict of $45 million in damages, apportioning 5 percent of the fault to Carmichael for an award of $42.75 million. The John Doe shooter and the man Carmichael met were each apportioned no liability.

"The next question most would come to ask, "Was this attack foreseeable and the apartment complex negligent?"

CVS claimed in their defense that Carmichael was not an invitee and thus deserved a lower standard of care. The appeals court disagreed. In the written opinion of the case, the court wrote that a "reasonable jury" could conclude that prior criminal activity made the robbery reasonably foreseeable. The judge wrote that Carmichael had no superior knowledge of the danger. The jury could determine that increased security or better lighting might have deterred the attack.

In a current case, scheduled to go to trial in September 2022, the plaintiff (we will call him Joey) pulled through the opened gates of the apartment complex. Joey pulled his car toward the back of the complex, near his apartment. There were shadows because the lighting didn't cover places potential hiding places for criminals.

Joey pulled into an open parking space. As he opened the car door, gunfire rang out. Bullets from two guns penetrated his car striking him. He ran in the hail of gunfire toward his apartment, collapsing on the sidewalk. The gunmen leaped into his car and made their exit. Seven .45 caliber and three 9 mm casings were recovered by police. Joey was severely injured—his legs would be amputated above his knees to save his life.

The next question most would come to ask, "Was this attack foreseeable and the apartment complex negligent?"

These cases illustrate a recent legal trend. Classifying security measures as amenities or courtesies may backfire when attempting to defend an apartment complex or shopping mall in a negligence lawsuit. Jurors expect landlords and property management companies to exercise a reasonable standard of care in protecting tenants from violent crime; the law demands it.

This article explores when prior crime makes the risk of criminal conduct against invitees unreasonable and foreseeable. The property owner and property management company have a duty to act reasonably to protect tenants and guests from such risks. Inherent in these cases is the concept of foreseeability.

FORESEEABILITY

A murder in Texas led to a precedent setting case in determining foreseeability. Luis Gutierrez in San Antonio, Texas, and his pregnant wife, Karol Ferman, went to a late movie at the Regal Cinemas at the Quarry Market, a 53-acre shopping mall managed at the time by Trammell Crow Central Texas, Ltd. According to the legal opinion, shortly after midnight, as the couple exited the cinema and neared their car, Ferman heard a shot. When she turned around, she saw the shooter, dressed in black with a black hood or ski mask over his face. Ferman did not think the first shot hit anyone, but she thought the shooter's second shot hit Gutierrez in the shoulder. Gutierrez fell to the ground, then got up, and the couple started running towards the south end of the mall. Then Ferman fell to the ground and, no longer able to move, got under a car. She never thought their assailant was shooting at her.

A subsequent autopsy revealed Gutierrez had been shot once in the back, twice in the back of his right shoulder, and once in the back of the head.

Gutierrez's mother Maria and Karol Ferman filed a lawsuit alleging that Gutierrez's death was proximately caused by Trammell Crow's negligent failure to provide adequate security. The jury returned a verdict in favor of the plaintiffs and awarded them $6.5 million in damages.

Most every state has legal standards that must be reviewed based on the location of the premises. As an example, in Texas, foreseeability of an unreasonable risk is analyzed by considering the factors described in the Timberwalk case. (Timberwalk Apartments, Partners, Inc. v. Cain, Supreme Court of Texas, 1998)

In Timberwalk, The Texas Supreme Court found that an apartment complex was not liable for the sexual assault of a tenant because the crime was not foreseeable.

In the written opinion of the case, the court noted that "the evidence in the present case is that no violent personal crime occurred at the Timberwalk Apartments for ten years preceding Cain's sexual assault. The only crimes that had occurred in the complex were the tire-slashing by Cain's roommate's ex-boyfriend, and a car burglary and car theft at an earlier, unspecified time. In the year preceding Cain's sexual assault, only one sexual assault had occurred within a one-mile radius of the Timberwalk Apartments. That same year, six assault-type crimes occurred in neighboring apartment complexes. There is no evidence that any of these crimes was ever reported in the media, or that Timberwalk knew or had any way of knowing about them."

The court also noted that the legal concept of foreseeability includes several factors—proximity of prior crime, recency of prior crime, similarity of prior crime, frequency of prior crime, and publicity of prior crime.

PROXIMITY OF PRIOR CRIME

Proximity refers to the distance from the subject property to the prior crime considered. The courts generally limit the radius one can consider in determining relevant crime. A plaintiff will have a stronger case when the crime data shows substantial and repetitive crime on the premises of the landlord. However, many courts allow a two-mile radius to establish proximity.

RECENCY OF PRIOR CRIME

Recency is the amount of time between the prior crime considered and the event at issue. A landlord or property management company has a stronger defense when the plaintiff is unable to show similar violent crimes in the past two to three years.

The court's imposition of a duty on Trammel Crow in the Gutierrez case rested upon its conclusion, according to the written opinion of the case, that "there is no doubt" that nine robberies and one aggravated assault over a two-year period at a 53-acre shopping mall were "'sufficiently similar' to Gutierrez's shooting" to render his murder foreseeable. It was thus irrelevant to the majority's analysis that none of the previous "violent crimes" involved a shooting (much less an injury from a shooting).

Likewise irrelevant to the majority's analysis was the undisputed evidence that the chance of being a victim of any violent crime (much less a murder) at that shopping center during the two years preceding Gutierrez's death was 1,637,630 to 1. The majority's analysis appeared to reject the Texas Supreme Court's analytical framework in *Timberwalk* and replace it with a rule of strict liability for premises owners.

SIMILARITY OF PRIOR CRIME

Similarity looks at the type of prior crime. Robbery, aggravated assault, murder, and rape are Part I violent crimes, accord-

ing to the U.S. Federal Bureau of Investigation (FBI) *Uniform Crime Report*. Residential burglary is also a Part I crime, and Texas courts have stated that residential burglaries are appropriate to consider when evaluating foreseeability of violent crime. Also, an appellate court noted that "property crimes may expose a dangerous condition that could facilitate personal crimes, as when apartments are targeted repeatedly by thieves," and "[b]urglaries, by their very nature, may suggest the foreseeability of violent crime." *(Jenkins v. C.R.E.S. Mgmt, L.L.C.*, U.S. Court of Appeals for the Fifth Circuit, 2016)

Auto theft and attempted auto theft are also similar to the crime where the victim was shot while being carjacked. Motor vehicle theft is also a Part I crime. Attempts to take vehicles may also involve violence, however, one should not limit similar prior crimes to the specific facts of the instant crime.

Joey was shot during a carjacking, which is an aggravated robbery. The expert for the defendant opined that none of the prior aggravated robberies, including those at gunpoint and those which were carjackings, were sufficiently similar to the shooting and carjacking of the victim, because no one had been shot. This narrow and restrictive view of similar crimes may be difficult to defend, because it is in conflict with most state laws.

The defense expert noted that he selected addresses for similar relevant crimes that were at or near the apartment complex. In fact, the defense report could have used a flawed method which made it near impossible to find similar crimes to include in his foreseeability analysis. The report omitted crimes directly in front of the complex and other apartment complexes next door. Rather, the report analyzed crimes at two churches, a daycare facility, and a dental office—all places that were extremely unlikely to have any violent crime.

At no point did the court in *Trammell Crow* indicate that it was changing the *Timberwalk* analysis. Instead, the court engaged in a typical Timberwalk foreseeability analysis and examined similarity of prior crimes. Prior violent crime at the entire 53-acre mall consisted of 10 robberies—three with guns and one with an unknown object that could have been a gun.

In distinguishing each prior crime, the court pointed out that the aim of the criminals was to obtain property, and three of the robberies were perpetrated on businesses—two stores and a bank—rather than individuals. The court also noted that no weapon had been fired, and no victim was seriously injured. However, the court focused on the extremely unusual nature of Luis Gutierrez's shooting, stating that "the circumstances of this attack are extraordinary."

The extraordinary circumstances were that the assailants opened fire from behind at long range without making any prior demand. After missing with the first shot, the attacker proceeded to shoot Gutierrez four more times from behind before taking his wallet.

The court further explained that the foreseeability requirement protects owners from liability "for crimes that are so random, extraordinary, or otherwise disconnected from them that they could not reasonably be expected to foresee or prevent the crimes." The court concluded that "the attack on Luis was so extraordinarily unlike any crime previously committed" the defendants could not have foreseen or prevented it.

FREQUENCY OF PRIOR CRIME

Frequency considers how often prior crime occurred during a time period in the area considered. The plaintiff has a duty to show that the frequency of similar crimes occurred over a specified period, such as two years. A case where there was one violent crime similar to the case in

question more than five years ago will make it difficult to show the frequency of violent crime on the premises.

For example, in a Florida case that was settled out of court, a woman we will call Mary and her 18-year-old son, Roger, decided to take a break after a long day moving to another apartment.

Along with two friends, Mary and Roger went to a Palm Beach, Florida, shopping center. They walked out of a restaurant micro-brewery in the shopping center after enjoying a meal. The parking lot was pitch dark. The only illumination was from the restaurant. As they got close to Roger's pickup truck, they noticed a woman dancing in the bed of the truck and two men jumping on the back bumper. The trio were loud and ignored Mary and Roger's request to get off the truck.

Suddenly, a female jumped from the bed of the truck and brutally attacked Mary. The men attacked Roger, breaking his leg. One of the men joined in the beating of Mary, slamming her head into the pavement.

During preparation for trial, the expert witness for Mary and Roger discovered that the shopping center had upgraded the lighting since the attack. The change in lighting was a fact the defense never disclosed. The expert found pictures of the shopping center that were taken months after the attack, which evidenced the sub-standard lighting. There were 197 crimes in the two years before the plaintiffs were attacked in the parking lot of the defendant's premises. Of these, 65 were suspicious incidents, persons, or vehicles; 41 were disturbances; 30 were unwanted guests; and 19 were assaults. The expert mapped the crimes in his 47-page report detailing his opinions of the negligence of the shopping center.

The parties agreed to a mutual settlement.

PUBLICITY OF PRIOR CRIME

Publicity of prior crime considers whether the property owner knew or should have known of the prior crime.

The expert for the plaintiff in Joey's case noted that the apartment complex knew about the crime that occurred on their property because the tenants informed them, the Houston Police Department informed them, their security guard informed them, and management received PIP (Positive Interaction with Police) reports, which listed all crime occurring on the property. The internal communication documents produced during discovery also demonstrated awareness of the crimes.

In the three years before the shooting of Joey, the Houston Police Department responded to the apartment complex 65 times concerning crime-related offenses allowed by Texas courts in laying the foundation for exemplary damages, or what is commonly known as punitive damages. Police responded to one non-family related murder. They responded to a total of 14 felony aggravated assaults, of which four were attempted murders and nine involved a deadly weapon. A police officer was also the victim of an aggravated assault. Police responded to 13 felony robberies in the complex.

Six of the robberies were classified with a deadly weapon. There was one sexual battery offense, along with seven terroristic threat offenses, two of which involved a firearm.

PREVENTION IS KEY

Prevention is the best tool to mitigate harm to tenants and invitees. Reasonable steps can help protect the property owner and management company from claims of negligence in the aftermath of a premises-related sexual assault, robbery, shooting, or murder.

Establish clear security policies and procedures, provide training at all levels, and take immediate and appropriate action when crime impacts the enterprise. Property managers should frequently audit the performance of their internal and contract security personnel. Independent risk

assessments that meet ANAB-accredited ASIS International standards are critical. Review law enforcement crime data and internal incident reports monthly. Sound security practices should never be marginalized or become an afterthought.

Lighting is another critical component of a sound crime prevention plan. Many county and municipal governments have regulations on the level of lighting for parking lots and commercial businesses. Moreover, ANSI has standards regarding minimum lighting levels. A common practice is mapping the property and recording light readings in foot candles. This type of record will become valuable evidence in the event of a future negligence lawsuit. Joey's attackers were able to take advantage of the heavy shadows.

If the enterprise has not equipped itself to perform a thorough and objective risk assessment, it often decides instead on labeling security as an amenity. This is a tremendous mistake. If made, the next time the business responds may be in a deposition in a costly and highly public negligence lawsuit.

STEVEN C. MILLWEE, CPP, IS A PROVEN EXPERT WITNESS FOR BOTH PLAINTIFF AND DEFENSE COUNSEL IN CLAIMS OF NEGLIGENCE AND BACKGROUND SCREENING. HE IS THE FOUNDER, PRESIDENT, AND CEO OF SECURTEST, INC., A BACKGROUND SCREENING AND INVESTIGATIVE CONSULTING FIRM. MILLWEE WAS THE 2002 PRESIDENT OF ASIS INTERNATIONAL. HE IS A FREQUENT EXPERT WITNESS IN PREMISES LIABILITY, NEGLIGENT SECURITY, AND BACKGROUND SCREENING CASES, AND IS THE AUTHOR OF NUMEROUS ARTICLES AND PATENTS.

How to Harden Security Infrastructure Against Attacks

Studies and industry security alerts have shown that most organizations do not sufficiently harden and protect physical security systems. Here's some guidance to get started on enhancing the security of your organization's security system assets.

By Bud Broomhead

Let's be clear: physical security infrastructure is the target of many cyber criminals. IP cameras, access control systems, visitor kiosks, and related systems are by their nature attractive targets because they have compute, storage, and networking (as traditional IT systems do).

But because they are Internet of Things (IoT) devices, the solutions used to secure IT systems simply won't work for them. Once breached, physical security systems can enable many other forms of attack on an organization, including planting ransomware, launching Distributed Denial of Service (DDoS) attacks, exfiltrating sensitive data, and potentially putting control of security systems in the hands of criminals.

Especially as the ability to create deepfakes based on real video footage becomes more sophisticated, ensuring

that physical security data is untampered and suitable to be used as evidence adds to the focus on hardening physical security systems.

During the last few years, studies and industry security alerts have shown that most organizations do not sufficiently harden and protect physical security systems. Just ask yourself: Are all your camera devices on the latest and most secure version of firmware? Are your device passwords maintained and unique in accordance with your corporate policies? Are any of your devices authenticated using 802.1x certificates, or having traffic between devices encrypted using TLS/SSL certificates?

If you answered no to most of these questions, it suggests that you're at high risk of your physical security systems being breached and exploited.

HARDENING SYSTEMS

Hardening physical security systems is hard! The starting point is identifying all the devices on your network, something that many security teams struggle with because of the scale of devices, their locations, and the long-lived nature of IP cameras. Whether using an IoT security platform that can do it for you, or by using a dedicated asset discovery solution, a complete inventory will drive all efforts in hardening those systems.

Consider making hardening your physical security into an industry issue: engage with others in your industry who share these same problems.

Another factor that makes physical security systems more difficult to protect is the heterogenous nature of such systems. Very few organizations have just one make

or model for cameras; most have several types, all with unique mechanisms for updating and securing them. Also complicating hardening devices is how they are often on isolated—or segmented—networks.

Reaching across multiple network segments to access the devices requires specialized technology, otherwise a lot of manual effort is consumed securing devices one network segment at a time.

Despite the barriers listed above, there are now more automated and purpose-built solutions to harden physical security—and in general IoT/OT—devices. The key functions of these automated systems are to:

1. **Implement firmware updates.** To remediate a known vulnerability, new firmware must be installed on cameras or access control devices at scale. Typically, this will need to be done multiple times per year as new vulnerabilities are detected and patches are rolled out.
2. **Enforce password policies.** As numerous CISOs have said before, "hackers don't break in, they log in." Preventing threat actors from exploiting default or easily guessed passwords means having a policy and method for ensuring strong, unique passwords are created and changed when necessary.
3. **Manage certificates.** Many organizations are moving to a Zero Trust approach, where independent authentication of the device is done to know whether to trust it. Certificates like 802.1x are used alongside a Certificate Authority to extend Zero Trust to physical security devices. This process needs to implemented and maintained.
4. **Assure service.** A functioning physical security system is critically important in stopping breaches; phys-

ically breaching an organization to plant malware or gain access to critical systems is a major organizational threat. Ensuring your physical security systems are always working will help reduce this risk.

BUILDING A TEAM

One advantage physical security teams have in implementing more rigorous methods for hardening their devices is that those systems are the most prolific and widespread IoT/Operational Technology (OT) devices in most organizations. As IoT/OT security becomes more visible at all levels of the organization, it is an opportunity for physical security organizations to take the lead corporatewide on IoT/OT security.

Since cybersecurity is a team sport, who should your teammates be? One best practice is to form an IoT Committee within your organization, with members from the CISO/CIO staff, as well as departments that manage IoT/OT devices like manufacturing, facilities, and logistics.

Organizations who have already formed such teams have also found an important side benefit: the processes used to monitor and harden physical security systems provide important data to other parts of the organization (compliance and audit, cyber insurance negotiations, public reporting, and so forth), increasing the strategic value of the physical security team.

By 2024, more than 75 percent of CEOs will be personally liable for cyber breaches, according to predictions and analysis from Gartner. Keeping your CEO and board of directors informed and aware of the efforts to harden physical security and IoT/OT systems will help to ensure that resources are made available to be successful in preventing cyber criminals from exploiting these systems.

Finally, consider making hardening your physical security into an industry issue: engage with others in your industry who share these same problems. During the last few years, several industry-level organizations—both existing and new—have made sharing best practices and information on threats more efficient and robust.

For example, the Real Estate Cyber Consortium publishes detailed information and guidelines on hardening and securing physical security and IoT systems specific to the commercial real estate business. Check within your industry if that exists or consider forming one because the types and methods of attacks will be similar across the industry and collectively the sector will be more resilient from that effort.

Whether through deploying automated cyber hygiene and service assurance solutions, documenting and sharing best practices, or fostering internal coordination across multiple departments, now is the time to take action.

BUD BROOMHEAD IS THE CEO AND FOUNDER OF VIAKOO, AN ENTERPRISE IOT APPLICATIONS MANAGEMENT COMPANY PROVIDING PERFORMANCE, SECURITY, AND COMPLIANCE.

SECURITY MANAGEMENT

ASIS INTERNATIONAL
Advancing Security Worldwide®

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

To join ASIS International and become a subscriber to *Security Management*, visit asisonline.org/membership/join.

GSX
GLOBAL SECURITY EXCHANGE

POWERED BY ASIS INTERNATIONAL

11-13 SEPTEMBER 2023
DALLAS, TEXAS, USA

MISSION POSSIBLE

Your mission: To assess evolving security risks and stay current on emerging threats. Presented by ASIS International, the premier association for advancing security, Global Security Exchange (GSX) brings together the best in the worldwide security industry to build and strengthen professional networks, grow skill-sets with CPE-eligible education, and collaborate on strategies to remain resilient against cyber and physical threats. Be there in person for the networking, connections, and tools you need to meet every mission.

REGISTER TODAY AT GSX.ORG