SECURITY MANAGEMENT

Facilities Security

A collection of articles on topics and trends affecting the security of facilities from the security industry's premier publication.

Powered by
ASIS INTERNATIONAL
Advancing Security Worldwide®

member appreciation month

SECURITY MANAGEMENT

How Facilities Security Has Changed

An interview with Dorian Amstel, CPP, PSP, senior director of physical security for DynCorp International.

Dr. Dorian Amstel, CPP, PSP is the senior director of physical security for DynCorp International, a U.S. government contractor supporting national security and foreign policy objectives. The company has 13,000 employees and has contracts around the world, including a high concentration in the Middle East. Amstel has been with DynCorp for three years and leads all site security operations worldwide: access control and CCTV systems, man-guarding, crisis management, travel security and Executive Protection. His security career spans more than 25 years and includes a seven-year post as regional security manager for Hewlett Packard, at which he oversaw security of HP's EMEA and Latin American operations.

In this exclusive interview for Security Management's ebook on Facilities Security, Amstel shares the knowledge and insights he has gained overseeing several different types of facilities in his career.

What types of facilities have you had under your security management?

I have run security for manufacturing sites for HP; Tier 1 data centers throughout Europe and Latin America, facilities with their own electrical grid; office buildings; research and development facilities; and more recently programs based on military bases, so it's been a lot of different settings. And each one is unique. Your security approach with data centers, for example, is going to be vastly different than security at a high-traffic facility like a manufacturing plant or multi-tenant building.

Can you describe some of the different security approaches required for different facilities?

Manufacturing facilities and office buildings are both high-traffic facilities, but how you secure each of them will be different. I was in charge of the security of a manufacturing plant in Puerto Rico. It was very high traffic—we had three shifts working one right after the other. It was running 24 hours a day. At a manufacturing site, you're concerned with theft of company property, so you have a very distinct procedure for securing valuables. When employees get to the site, they would have to secure their valuables, lunches, personal items, before going onto the manufacturing floor. And when they come out, they could not leave with anything from the manufacturing floor and so you have to screen for that. An office building is likely mostly vacant for large stretches of time, and people expect to take their bags and personal items into their workspace, so your security priorities in that environment will be totally different.

What is your approach for frontline security guards?

One thing I've tried to do is consolidate outsourced security suppliers. Ideally for any region, you'd like to get a single vendor for all the various countries in which you have facilities, but realistically that's not possible. Even the large players don't have that kind of footprint. However, by consolidating as much as you can, you can gain some economies of scale. When you have a large operation with dozens or hundreds of different sites, your bill just for guard force will easily get into the millions.

What is the process for contracting for such a large guard force?

We would start with RFPs outlining all of our sites and all of our shifts. We would list everything we had in place in terms of equipment, be it radios, vehicles for the guards, or whatever else we needed. We would outline the shifts and the level of officers, from basic guards to front desk guards to operational supervisors.

From there we would detail the statement of work to be joined to the contract and later post orders for each site. You start with a boilerplate post order detailing the basic job tasks, and then the post orders are tailored to the site depending on the specific needs of that site. And then your supervisors are working with the guard supervisors, so these things are continuously updated, and when it's time to conduct a new RFP, whether you're renegotiating a renewal or opening a new facility, you're ready to go.

Other than guards, what systems are important for facilities security?

Most sites will have some kind of access control solution. For badging, most companies are using proximity cards, the old Wiegand cards, and that's a problem because they're generation 1990. With a device you can pick up for $15 on Amazon, you can clone a first generation proximity card quickly and easily. Though few have done so, companies should move to the iCLASS level of badging, where the readers themselves, as well as the badges, are encrypted. Upgrading would, of course, have a cost associated with it, and many sites have a ton of those old proximity readers, so it can be cost prohibitive to change them all out.

And then you've got your video. There's a lot of talk about the Chinese companies providing video systems, with people worried that the systems leave back doors open that enable the Chinese to spy on your operations. As a defense contractor, we don't use any of that. The McCain Act prevents us from purchasing anything that is Chinese made. The video technology has undergone drastic change as we moved from analog to IP cameras. Old equipment like video matrix are a thing of the past, it's all done through software platforms, and there are a lot of added capabilities.

You can even activate a crisis team directly from your phone, even if you're hiding in a bunker, as long as you have connectivity.

And going further, notification systems have improved tremendously from what they used to be. Back in the old days, if you weren't at your computer when something suspicious happened, you weren't sending any messages. Today, all these systems have capability to send messages directly from smart phones. You can even activate a crisis team directly from your phone, even if you're hiding in a bunker, as long as you have connectivity. This is a big plus when it comes to our response capabilities. You can have your entire team from around the world on a conference call in minutes.

These systems show how far we've evolved from the old "guards, guns, and gates" days. The classic way of looking at securing facilities still applies: you start with your perimeter and you look at concentric rings of security. It's just that with better equipment and updated procedures to take advantage of the equipment you can see more, prevent more, and react quicker.

Can you give an example of how security has been enhanced?

One way is that within facilities, companies are realizing they can segregate certain spaces. I run a lot of checks on access controls to see if people are trying to access places that they shouldn't. The systems now allow you the capability to see what people are doing within the site. And, of course, then you also get to add enhanced security to places that are more sensitive.

Also, using architectural structures in your security has grown in use and importance. For most existing facilities, your options are going to be limited, but there are often some enhancements that can help protect a facility from some kinds of threats. And if you're building a new facility, now security is much more involved with global real estate. We start with more input than we previously had, so we can design security into facility from the start. CPTED, also known as crime prevention through environmental design can be applied with more ease at new facilities than on buildings which are already built.

What are the factors driving security change?

Gone are the days where you leave your car unlocked in the parking lot, or you don't lock your front doors or you don't leave your computer untethered to your desk. Corporations in general are much more security minded, and employees themselves are much more security minded.

At HP a tremendous challenge was theft of laptops. It wasn't the physical costs of the laptop that was the problem, it was what might be on that laptop from client data to product data or whatever else might be on there.

There's been an evolution of security awareness. And a lot of it has to do with some of the certifications that have become more of the norm and that your customers require that you have. For instance ISO 9001, ISO 20001, or the hundreds of other certifications required in different sectors, for example in the banking industry, the certifications you must have in order to handle client data—there are physical security requirements critical to achieving all of these certifications. Everything has kind of come to a head: we are in a world where we need to be more secure about things, and now suddenly we've got requirements we need to fulfill if we're going to be competitive.

Security used to be like HR, where the minute they walk through your door, you'd think, "oh man, am I getting fired or what am I going to have to do now that I don't want to do." Security was also seen as a cost center. Do we need all these guards? Do we really need to upgrade this system? Today it's very different. I'd go so far as to say we almost generate revenue because we do the things that allow companies to get the certifications their clients require. It's a been a combination of all of these things. From your lighting to signage, they all work in your comprehensive security program, so there has been a huge change over the years.

What else has made a significant impact on facilities security?

Guard companies have become more professional. There's been a push by many organizations, including ASIS, to move away from the view that private security guards are failed cops or old retirees. The security workforce is more professional, and it has come through development of training programs and through setting standards. A lot of the large guard force companies seek or require former military training. All of this has led to a much higher quality guard. That's not to say that we're there by any means—particularly on a global scale. Part of the issue is tied to wages and costs. We all want to pay as little as possible when we're hiring outsourced positions. But you can't require more professionalism and more versatility and not expect to pay for it.

Can you describe a typical security incident and how you go about learning from it?

This was a few years ago, at a large site in Costa Rica. An individual was sitting at his desk and saw a little packet. He pulled at it and a bunch of dust flew in the air. The individual next to him started having breathing issues, and a bit of a panic started to set in because they thought it might be a chemical agent. This prompted the site supervisor to contact his boss, and we activated the incident management team. We shut down the HVAC system and the police and fire and rescue showed up expecting a possible chemical agent. It was chaotic. It turned out it was one of those little packets you put next to electronic equipment to prevent moisture damage. The person experiencing breathing issues had severe asthma, and just the particulates from the packet in the air was enough to initiate some respiratory distress. So it was a serious, chaotic false alarm.

We learned several things. First our reaction time was not as quick as it needed to be. We needed more training when it comes to things like involving global real estate to shut down an HVAC system to prevent powder or dust from being spread around a building. We also realized that we were lacking in response when it came to the capabilities of the first responders. They came in and were not really prepared for an incident involving a real chemical agent. They weren't suited up in protective gear and they entered the affected area, even though the situation was described to them. There may be very little we can do to impact the outside environment, meaning the first responders. In the U.S., it probably would have been different, so that is going to vary quite a bit by country.

We started incorporating other functions into the process and training them and ensuring that information flowed quickly and accurately to try to cut down on the chaos.

One of the things we changed as a result of the incident was the makeup of our emergency team for activation in such eventualities. We started incorporating other functions into the process and training them and ensuring that information flowed quickly and accurately to try to cut down on the chaos.

What are the changes you've seen have a big impact on security?

The first thing that comes to mind is what we talked about earlier: the enterprise's view of security has changed. Security is now far more involved with every facet of the organization and has C-Suite support. We're in a more uncertain world where failures in security are more costly for our enterprises and our environment is much more regulated. Security is much more of an essential partner for the rest of the enterprise.

I think the other thing that has benefited security as a whole is the improvement in systems and the drop in price of sophisticated electronics. It's akin to flat screen TVs: ten years ago you had to pay $8000 and now you can get a 55-inch with a better picture for $300 at Walmart. The cost of electronics has decreased and the availability of systems to help you do your job has improved. This puts less strain on companies of all sizes. Good, basic security solutions are within reach of even the smallest companies operating with tight margins.

What are the changes you'd like to see?

I think while organizations do the basics—they have access controls and video surveillance and guards with post orders—as a whole they are missing an opportunity by not having an enterprise risk management approach to their business. Individual business units might have some kind of crisis response, but when it comes to business continuity and testing what they have in place to continue operations across the enterprise in times of crisis, to be resilient, I think there's still a lot of room for enterprises to improve.

Here's a small example: When I was with HP, the call centers that handled all customer support for France had a complete system shut down, so they were not able to provide customer support at all, which was a big issue. The company was able to flip a switch and all customer support calls were picked up in Tunisia to overcome the language barrier. This did not come about by mistake. The company had prepared for such an instance and practiced it. Many companies wouldn't do that. They won't simulate the shut down of an entire site to see the effect it will have. The reason they don't do it is there's a price tag associated with that, but often the price tag of not doing it could be catastrophic.

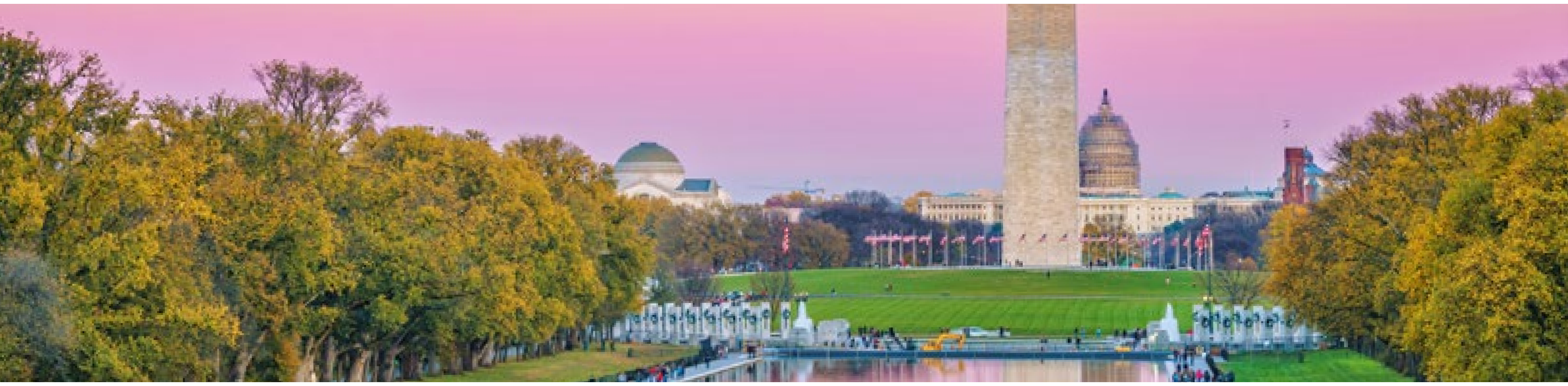
The other thing I'd like to see is licensing reform at the state level in order to make it more difficult for folks to obtain security guard licenses. I think that right now for regular security guards, most courses might run for a week. For armed security guards there will be one course of fire, and they won't be required to do anything else for a year. And that ties into the individual states and countries in terms of requirements they have for people who will have those licenses. But we're in a tough situation there; if we suddenly make it more difficult, will we put pressure on guard force suppliers to increase prices and would we be prepared to increase our own costs? But I do think the industry could benefit from a guard force that continues the trend of being more professional.

SECURITY
MANAGEMENT

Security by Design

In the U.S. capital, architects use CPTED best practices to keep visitors safe while addressing many other design challenges.

By Lilly Chapa



If you look closely, you'll start noticing it everywhere: the long, brightly-lit walkway with well-maintained vegetation along the sides, the line of stone benches running along the perimeter of a building in a popular tourist area, or the Instagram-worthy sculptures and architectural elements thoughtfully placed throughout an urban park.

These carefully constructed public spaces have components designed to delight and enhance the experience of the people who use them—but they also employ natural security techniques honed over decades to subtly create a safer space for all.

This approach, known as crime prevention through environmental design (CPTED), was first introduced in the 1970s and has steadily gained popularity since. Today, CPTED is a common component of physical security and architectural design—and for good reason. Urban areas are constantly evolving to support the influx of city dwellers; more than half of the world's population lives in urban areas today, and that number is expected to increase, according to the United Nations. That growth, combined with the recent increase in soft target threats such as vehicle attacks and mass shootings, makes security in densely populated areas crucial.

However, the challenges faced by security practitioners to harden public spaces are numerous—the cost, the difficulty of retrofitting an existing area with new physical security components, and the implications that come with an increased visible security presence. This is where CPTED is especially useful, says Mark Schreiber, CPP, principal consultant of Safeguards Consulting, Inc., who is involved in ASIS standards development and multiple councils.

"CPTED is a whole other set of tools where we could apply security design to facilities but, instead of applying technology or a specific hardware, CPTED addresses overall facility design itself," Schreiber says. "It's important for security design aspects to be teaming up with other types of design—with landscape, civil, and structural engineering and physical security technology. We're changing the physical environment that a human goes through and influencing the human's behavior through those designs themselves, whether it's outdoors or indoors, because that environment influences behavior naturally. People know when they feel safe, and a criminal knows where they're more likely to get away with a crime because of the environment."

While the basic principles of CPTED outlined in the 1970s remain the same today, they have become more nuanced—the approach is a careful balance of physical security, architecture, psychology, and perception. Successful implementation of CPTED components in public areas requires equal input between the landscape architects who are designing a layout and the security principles needed to build a safe environment.

> ***“We always keep in the forefront of our mind that dichotomy and our obligation to ensure that when visitors leave these landmarks that they’re not taking away a sense of foreboding.”***

But for landscape architects, security is just one component of a larger plan. They also need to consider accessibility, aesthetics, municipal requirements, and resiliency—all of which need to be incorporated into one solution. While security and urban design often have differing—and, at times, clashing—approaches to how public spaces should be protected, the final result, when done well, is a seamless experience that leaves visitors feeling at ease.

“There are these fantastic themes of visitor use and experience, as well as public safety,” says Jill Cavanaugh, a partner at Beyer Blinder Belle Architects & Planners (BBB) in Washington, D.C.—a city full of national landmarks and tourist attractions.

“We always keep in the forefront of our mind that dichotomy and our obligation to ensure that when visitors leave these landmarks that they’re not taking away a sense of foreboding—you want them to feel safe and protected, but you don’t want to have that experience diminish their overall enjoyment of these landmarks,” says Cavanaugh.

DESIGNING A MALL FOR THE PEOPLE

Cavanaugh and the architects at BBB have plenty of experience designing for some of the United States’ most stringent security requirements—following 9/11, they were tasked with increasing the safety of several national landmarks, including Smithsonian Institution museums, many of which line the National Mall in Washington, D.C.

"Because of the nature of the public spaces, monuments, and important buildings within the city, they all became vulnerable in so many ways, and there was a big need for them to be protected," explains Hany Hassan, partner and director of BBB's Washington, D.C., office. "We developed a comprehensive plan for the entire Mall with the intention to provide necessary security while being mindful of the quality, aesthetics, and historic nature of those buildings. We had to do it in a way that wouldn't compromise the Mall's symbolic nature of openness, freedom, and accessibility."

While security in the design was a top priority due to the buildings' locations and symbolic importance, the architects had to keep other design aspects in mind.

"Our approach has to be dynamic enough to accommodate the things that oftentimes we can't control," Cavanaugh says. "The buildings in which we work are in dense urban areas, so we don't have the luxury of a setback. How do you appropriately harden a building physically in a way that honors the aspects of the building that make it significant? We really maintain what makes the building special from a historic or aesthetic point of view, but [we] incorporate measures that are often invisible but do include the appropriate amount of structural resilience and electronic intrusion resistance."

Scott Archer, a senior associate at BBB, tells *Security Management* that urban plans often incorporate a layered security approach, which is both more effective and less noticeable, ensuring that organizations are not relying on a single line of defense to stop all threats.

"The new visitor pavilion we designed for the Washington Monument isn't designed to protect against a vehicle ramming, because that's being protected against elsewhere," says Archer. "This layered approach not only helps the user feel safe while still navigating those spaces with ease, but also allows the security apparatus to actually defend against things in a more discreet way. You can't make it completely transparent in the way that it's designed because you don't want others to know what level of threat it's designed to. It's about the balance between allowing people to feel safe knowing that they're protected without describing the level of protection."

"This layered approach not only helps the user feel safe while still navigating those spaces with ease, but also allows the security apparatus to actually defend against things in a more discreet way."

The results of BBB's approach can be seen along the Mall today—but only to the careful observer. That marble ledge that's the perfect place to sit while waiting in line to enter a museum also serves as a retaining wall and a barrier. The eye-catching sculpture that marks the entrance to the Smithsonian Institution's National Museum of American History is reinforced to act as a bollard. A facility's intricate wooden entryway may house a magnetometer. And there are many design components that meet strict federal security requirements and are almost impossible to detect—a slight slope of the sidewalk, unimposing vegetation, or a carefully placed trash can far from a building's entrance.

"One of the best compliments we have received on this kind of work is that people didn't even notice that there is perimeter security," Hassan says. "When we do any of these projects, it's not an exercise of flexing our muscles in designing an elaborate system—we want it to be nearly invisible."

Internationally, though, the design approach might be less subtle. Cavanaugh, who leads many U.S. State Department projects overseas, explains that sometimes a facility's security features should be showcased, not hidden.

"On these campuses, we always have perimeter security that looks like perimeter security, so that there's a definite visual message to any visitor, whether friendly or unfriendly, that this is a protected U.S. military installation, even though it's a diplomatic presence," Cavanaugh says. "It's important to emphasize security as a visual element but also have that diplomatic layer of encouraging visitors whose only interface with the United States might be through that post."

A TEAM APPROACH

As CPTED best practices have become more widely understood throughout many industries, it is easier to work together to make design decisions among a multidisciplinary group, Schreiber notes.

"The great thing about CPTED is that it's not a big lift—it's relatively simple to implement because there's not a lot of friction with the design process when you have trained professionals in the group," Schreiber says. "Ultimately, it requires a team approach, proper education, and experience to implement CPTED. Common CPTED training programs educate a wide variety of people—security engineers and consultants, managers, architects, law enforcement professionals, and city planners. What it comes down to is that the principles are applicable to many different physical environments, including the built environment, and whoever is influencing that environment can use it in that case."

Cavanaugh agrees, noting that the interactions between architects and security professionals often have a healthy tension to them that can result in innovative solutions that will satisfy everyone.

For example, Cavanaugh says: “If you have a challenge where you need a certain perimeter distance for a vehicle, there are many different ways you could work with the landscape to accomplish the same security objective. Those are some of the most fruitful dialogues because security professionals might perceive the solution to be a wall or fence, but there are other ways to address the issue and how to resolve it.”

Schreiber notes that ASIS is working with the International Organization for Standardization (ISO) to develop internationally agreed upon guidelines for CPTED best practices.

“We have made significant progress in making this standard into something that can be practically applied to any organization, including main CPTED principles and guidance that can be implemented,” Schreiber says.

EVOLVING WITH THE INDUSTRY

Hassan says that the changes in physical security technology and the threats facilities face influence how the architects incorporate security into their designs. The evolution of x-ray and other screening technology, for example, allows architects to incorporate those security measures into the facility more seamlessly for clients seeking to create a more welcoming environment, he adds.

“The equipment is no longer as unsightly or intrusive, but more importantly we can now make the building more inviting when you enter, as opposed to being confronted with equipment when you step in the door,” Hassan says.

The constantly changing threat landscape is a challenge, especially when designing for a historic building that can’t be completely revamped to address new security concerns, he notes.

“What we hear from our clients is to design to the threat, but that’s always evolving,” Hassan says. “As much as we are trying to improve the systems and equipment we use, at the same time others trying to do harm are coming up with new ideas and ways to surpass that. It's a constant challenge and competition between everybody to be able to protect ourselves from anyone trying to do any harm."

"When we're designing places, whether it's an urban landscape or a building, often these are giant monetary and time investments, so they usually aren't temporary."

This is where resiliency in a building's design is especially important.

"When we're designing places, whether it's an urban landscape or a building, often these are giant monetary and time investments, so they usually aren't temporary," Archer explains. "Think about the longevity of an embassy overseas—that should ideally last for more than 100 years, but then the threat will be completely different. How we design in flexibility is really important, and we do that not just for security but for all types of issues within the building. We try to think about our master plans and our urban design as an exhibition of how this can come together in a way that makes sense for today and lays the landscape for how it might change over time without having to restart every 50 years."

When it comes to resiliency, the architects take a holistic view about the mark they will make on structures that have existed for hundreds of years and, hopefully, will continue to serve the public for years to come.

"Solving security in design is one-dimensional, and when the threat changes it becomes antiquated," Cavanaugh says. "If it's solving more than one problem, though—if we're layering in an infrastructure upgrade, bringing the building out of the flood plain by raising it 30 inches, and also accomplishing a vehicular barrier and incorporating accessibility—all of these things make design more resilient to both time and purpose. That's where we find the most enjoyment: a multidimensional design that solves more than one problem in a way that's sensible but also intuitive and will be more enduring in the way that people use it in the years to come." ▨

LILLY CHAPA IS A FREELANCE WRITER COVERING THE SECURITY INDUSTRY AND A FORMER SECURITY MANAGEMENT ASSOCIATE EDITOR.

SECURITY
MANAGEMENT

Guard Force Trends: Multipliers and the Market

Technology, market forces, and other factors have transformed security guard forces and their management. Here's a tour of some of the latest challenges and best practices.

By Joseph Ranucci, CPP

Security guard forces, and the methods used to manage them, have seen transformational change in recent decades. Twenty years ago, the tools of the trade were a notepad and a pen, and the required technical skills peaked with the ability to use a handheld two-way radio. Guard force security was not viewed in a professional manner; guard jobs were often considered "no specific skills needed" entry level positions. Recruiters frequently told applicants, "If you can stay awake, you can do this job."

Now, advances in technology and market forces have significantly changed how a guard force works and is managed and have also changed the role of the individual guard. These changes, which in turn have helped transform the employment economy at large, have ushered in a new business model for many guard forces.

TRANSFORMED BY TECHNOLOGY

Security guards are no longer limited to positions like overnight officers conducting patrols in empty buildings, Checkpoint Charlies sitting in booths, or watchmen hidden away in a back room monitoring security cameras. Many security guards are now stepping into the light to serve in more customer-facing positions.

This trend is due in part to the spillover effects of market growth. The frequency of mass shootings in public places, continuing concern over terror attacks, and increasing crime rates in some major cities have all spurred growth in the security guard force industry. Due to this growth, guards are more commonplace in corporate offices, residential facilities, and schools.

With more guards in these settings, it's not unusual for security guards to fill in as receptionists or concierges—often the first point of human contact for visitors. This new role brings with it a new set of skill requirements, such as customer service ability, proper phone etiquette, and a certain level of computer proficiency. Requirements for the latter continue to rise as the available technology continues to develop.

Guards serving as concierges and receptionists will typically be responsible for access control and visitor processing. But the visitor processing protocol has changed. Today, most access control systems offer a visitor management option or the ability to interface with a third-party visitor management system.

Rather than record visitors in a log book and issue paper passes, the technology is now available for visitors to be registered and recorded in a database. Guards may need to use digital cameras to capture photos and print temporary passes. Scanning IDs to perform instant background checks is becoming more common. These tasks require the guard to have a higher level of technical proficiency than was needed in the past.

These access duties are just one example of how technological advances have transformed guarding. Token-based touring systems, which record data electronically into hand-held units that are downloaded into a central database upon completion, have been the industry standard for decades. But with new technological innovations, handheld downloadable tour systems are quickly being replaced by smartphone-based tour systems.

With new technological innovations, hand-held downloadable tour systems are quickly being replaced by smartphone-based tour systems.

These new systems allow for real-time reporting and have enhanced reporting features, providing greater detail than the download systems. They use either QR codes that interface with a smartphone's camera or near-field communication (NFC) technology, which allows the smartphone to scan tokens around the facility.

MANAGEMENT CHALLENGES

With these changes in technology, managers must realize that not every guard will be able to gain the needed skill sets. For instance, after starting in his current position in early 2018, the author began to evaluate the tasks being performed by contracted security staff. At the time, they were still almost exclusively providing pen and paper reports and logs.

The author implemented some modest changes such as moving to typed and emailed incident reports and allowing the guards use of the access control system to check employment status of individuals, issue temporary badges, and do some low-level troubleshooting.

Most of the guard staff were able to take on the new tasks, but two individuals ended up lacking computer proficiency to adapt to the changes. Although the guards were reliable, well liked, and had other positive traits, their inability to adjust to the new technical requirements forced a change in staffing. This was not a decision made lightly, but in the end the guard service provider recognized that requirements now exceeded the individuals' abilities and that changes were necessary.

Technological advances can also create other types of challenges for those managing a guard force. Take, for example, the diverse smartphone touring systems, many of which incorporate GPS tracking and geofencing to ensure that the guard conducting the tour is in the proximity of the token (or QR code) being scanned.

In one instance, a guard force manager set up a QR-code-based tour for a client site. Unfortunately, the manager did not fully understand the functionality of the system, so he did not activate the GPS features. A resourceful security guard working for the manager realized that he could conduct his entire tour by taking photos of all the QR codes and then printing them onto a single page. Using that single page, the guard then scanned the codes one at a time—all from the comfort of the office.

Since the reason for the tour was to inspect the areas of the facility for hazards, including potential chemical leaks, the guard's decision to improvise and skip the tour was risky. As it happened, a leak did occur at the site, which is how the guard's malfeasance was discovered. Fortunately, the leak was minor, and no damage occurred. Still, the guard company was penalized and required to pay the cost for the modest cleanup.

Once the problem was discovered, the manager came up with a solution. The QR codes were all replaced with

NFC tokens, which require the smartphone to be placed just inches from the token to record the scan. This eliminated the possibility that another guard might conduct stationary tours.

MANAGEMENT ENHANCEMENTS

As the prior example makes clear, innovative technology alone does not solve all issues. The technology must be understood and used correctly to bring about process improvements.

Many other areas of guard force management have seen advancements due to new technology. Software applications, smartphones, and various other pieces of hardware and software have all become essential management tools.

Timekeeping. Timekeeping apps for real-time attendance allow managers to know exactly when guards report to duty. This has several benefits. It is important for wage and hour compliance, and it helps supervisors manage cold start positions, positions where the arriving guard is the first on duty and is not relieving another officer, by sending an alert if a guard does not arrive on time.

For example, a guard company with a significant national presence in the high-end retail market operated cold starts at most of its locations. To avoid client-imposed penalties for late arrivals or open guard posts, the guard service company needed a system that would provide real time information.

Rather than having every guard individually call into a central dispatch, the guard services company decided to move to an automated system. In the new system, guards would call into an application and enter a PIN code, which allowed them to either check in or check out. The system verified that the guards were on location by using GPS and caller ID. This meant that dispatchers no longer needed to take dozens of calls at the start of each shift; they simply had to monitor the control panel to ensure that each post had a proper check-in. Late and open posts triggered an automated notification to management.

As a management tool, this system proved effective. Guards could no longer call into dispatch claiming to be on site, while they were still 10 minutes away from the location. Dispatchers were not bogged down for 15 minutes taking an onslaught of calls. Guard arrival times were recorded more accurately because they did not have to wait in a queue for the dispatcher to take the call. And in the event a guard did not report on time, management was able to respond faster to meet the clients' needs.

Tracking vehicles via GPS is not a new practice. But now, with the use of smartphone apps, guards inside a facility can be monitored in the same way vehicles have been tracked. With accuracy within a few feet, GPS can track a guard inside a facility, and an app can report back to management if the guard remains stationary beyond a designated length of time.

GPS can track a guard inside a facility, and an app can report back to management if the guard remains stationary beyond a designated length of time.

Although this option is often used to detect if a guard has fallen asleep, it can also serve as a health safety tool. Since many guards work alone, an alert indicating that a guard has been motionless for a certain amount of time can be valuable in the event a guard becomes injured or incapacitated while on duty.

Inspections. Another management responsibility assisted by technology is guard inspections. Management can visually inspect guards when they are not physically on-site using apps such as Skype or Facetime.

The use of a webcam provides higher quality inspections versus simply checking in by phone. A guard's appearance, uniform, and post can all be visually inspected to ensure compliance with company standards. This improves overall efficiency by eliminating travel time between facilities and allowing significantly more guards to be inspected during a shift.

RECRUITING

In the past, guard force companies commonly took an assembly line approach to recruiting, with the next person in line assigned to the next available opening. But this put-a-body-on-a-post mentality didn't significantly consider an individual's abilities or the requirements of a specific job.

This approach often resulted in a security guard shell game, with guards rotated from client to client whenever problems occurred. Rather than separate from problem employees, guard companies would simply transfer them to fill a vacancy elsewhere. Some guards passed through half a dozen sites or more before the company finally terminated employment.

The mission of today's recruiter is to be more selective in identifying the right candidate for the appropriate position. Often, it must be determined whether a candidate has the technical skills to use the needed hardware, mobile apps, information databases, and various software applications. Besides technical abilities, security recruiters are also looking for customer service and communication skills. Many openings seek candidates with at least an associate degree, or equivalent work experience.

Overall, the emphasis is on making sure the individual fits the job requirements. A candidate with outstanding customer service skills may make a great concierge. But if he or she does not have strong computer skills, that same candidate may not be a good fit for a security command center position.

Complicating the security recruiter's job is that other industries that have traditionally hosted many minimum wage jobs have begun changing their business models and increasing their base wages well above state mandated minimums. For example, Amazon has established a $15 minimum wage, Costco $14, and Target and Walmart are both at $11. This creates competition for employees as the wage gap between security positions and other entry level jobs closes.

Guard force recruiting is also affected by the low U.S. unemployment rate. In November 2018, the national unemployment rate held at 3.7 percent, the lowest jobless rate since December 1969. When unemployment rates drop to such historic lows, qualified personnel become more difficult to find and hire, especially with increased competition from other industries.

When unemployment rates drop to such historic lows, qualified personnel become more difficult to find and hire

To contend with these difficult conditions, security recruiters are more aggressively developing internal talent pools, holding onto applicant résumés longer, and using online resources to proactively seek out candidates. As the traditional candidate pool shrinks, recruiters are looking toward recent college graduates and returning military personnel for skilled job candidates.

The author experienced firsthand how tight the labor market was in the scenario cited previously, when the two guards were let go because the job requirements grew beyond their capabilities. The author recognized that the additional job responsibilities should come with higher compensation, so when the changes were rolled out the company also implemented a 25 percent pay increase for the remaining guards.

When the company advertised the two open positions at the higher pay rate, it could not quickly find qualified replacements. Although the company still maintained its contractual guard requirements and never dropped coverage, it did so by absorbing non-billed overtime for several months. It took a significant loss to its profit margin.

PERSONNEL MANAGEMENT

Guard force management is, at its root, personnel management. And so, management issues that arise from human resource-related concerns deserve serious consideration.

In U.S. states such as California, which has extremely stringent wage and hour requirements, mismanagement can expose a company to class action litigation. In recent years, several guard service companies have had multimillion dollar judgments awarded against them for violations. Technological solutions like the call-in system discussed previously can help, but like any other tool they must be managed and used properly to provide a benefit.

In the #MeToo era, employees today are more informed and aware of their rights, and information and resources are just a Google search away. U.S. Equal Employment Opportunity Commission (EEOC) and harassment complaints can bring with them significant financial penalties to the individual manager and company. In today's business environment, good managers have a strong understanding of what behavior and conduct constitutes, or approaches, harassment from an HR perspective.

Just before the #MeToo movement made national headlines, one guard company was being served with an increasing number of EEOC and harassment complaints. In a meeting with the CEO and vice president of human resources, the CEO suggested increased training. This initially seemed like an excellent suggestion, because it would help managers in their interactions with employees and raise awareness of key HR issues.

But then the CEO clarified his suggestion: he indicated that the training he wanted was for the guards to understand "that it's not illegal for your boss to be a jerk." It became clear that there was a top-down management problem. The CEO's attitude clearly did not fit with current thinking about sustaining a healthy workplace culture.

"The line between disrespect and harassment is very thin," said Matt Verdecchia, a senior trainer with Health Advocate's EAP+Work/Life division, during the Society for Human Resources Management's 2017 annual conference. "We need to be more sensitive to insensitivity."

Clearly the CEO of the firm was not being sensitive to insensitivity. Managers must understand that their attitudes have consequences, and the more senior a manager, the greater the impact. Complaints against that company continued.

"The line between disrespect and harassment is very thin. We need to be more sensitive to insensitivity."

In the past, a guard force manager's interaction with HR typically began and ended with recruiters. Today, a successful guard force manager should embrace the broader role that many HR managers have taken on in companies. EEOC education and antiharassment training should be a part of every guard manager's core curriculum. Maintaining open communication with regards to employee coaching and performance evaluations can avoid costly situations.

Guard force operations and management will continue to change. New technologies are developed, the economic landscape evolves, and new challenges emerge. But at the end of the day, a guard force consists of individuals. For senior managers down to the on-site guard, change will be continuous. In response, education, training, and learning from experience should be, as well.

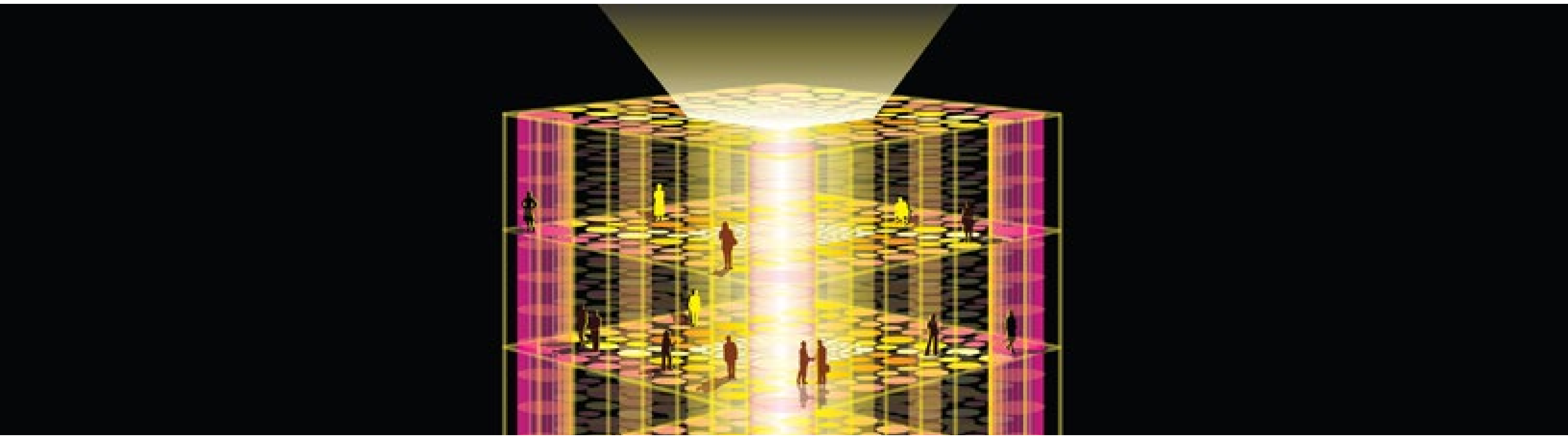
JOSEPH RANUCCI, CPP, IS THE U.S. MANAGER OF SECURITY FOR ALMAC. HE SPENT 15 YEARS WORKING IN MANAGEMENT AND EXECUTIVE POSITIONS FOR MULTIPLE GUARD SERVICE PROVIDERS. RANUCCI BEGAN HIS CAREER IN 1993 WHEN HE WORKED AS A SECURITY GUARD WHILE EARNING A BACHELOR'S DEGREE IN CRIMINAL JUSTICE.

SECURITY MANAGEMENT

Smarter Structures, Safer Spaces

Buildings are alive with functionality, but security is often overlooked when it comes to a facility's control systems. A report sponsored by the ASIS Foundation outlines what security practitioners should know.

By Dave Brooks and Michael Coole



Internet giant Google is known to build impressive campuses and office spaces for its workers. No exception is its Wharf 7 office in New South Wales, Australia, where it moved a number of employees when the company experienced a boom in growth in 2012.

The building was constructed to "encourage the interaction and collaboration that is key to the innovation Google promotes," IDEA Awards, an interior design awards program, states on its website. A gaming room, café, bridges, and walkways all contribute to the collaborative look and feel of the building.

While the interior design of Google's Wharf 7 is impressive, two security vulnerability researchers discovered that the system controlling much of the building's functionality had not received as much attention.

Billy Rios and Terry McCorkle, both of security firm Cylance, gained access to the corporation's building management system, a computer-based system that controls electrical and mechanical functions within the facility. They achieved this breach by exploiting unpatched vulnerabilities. In other words, they accessed the network that controls HVAC, lighting, fire and life safety systems, and more, because Google had not run security updates on some of those platforms.

"Among the data they accessed was a control panel showing blueprints of the floor and roof plans, as well as a clear view of water pipes snaked throughout the building and notations indicating the temperature of water in the pipes and the location of a kitchen leak," according to a May 2013 *Wired* article.

Upon learning of their research, Google promptly patched their systems and thanked the white-hat hackers for their warning. The lessons learned have far-reaching effects for facility and security professionals as they navigate their buildings' complex automation and control system environment.

INTELLIGENT BUILDING MANAGEMENT SYSTEMS

Intelligent building management systems (IBMS) are embedded in most contemporary buildings. IBMS continue to grow by anywhere from 15 to 34 percent each year, according to a report from revenue intelligence company MarketsandMarkets. Such growth is due to the demand for reduced operating costs, improved information flow, greater sustainability, and meeting increasing government regulation in building ownership and operations.

By 2022, it is estimated that the IBMS industry will be worth approximately $104 billion, according to a study by Transparency Market Research. However, this technological enhancement comes with a substantial set of security vulnerabilities that many facility and security professionals have not accounted for. As the Google example shows, if the security of IBMS is not considered, organizations will remain exposed to harm from nefarious actors.

Vulnerabilities. The security vulnerabilities associated with IBMS stem from their incorporation across the built environment. IBMS integrate a building's operational management systems, such as HVAC, lighting, and life safety systems. They are also integrated into security systems, such as intruder detection, access control, and surveillance systems.

The security vulnerabilities associated with IBMS stem from their incorporation across the built environment.

A detailed research project, funded by the ASIS International Foundation, the Building Owners and Managers Association (BOMA), and the Security Industry Association (SIA), recently investigated the security of IBMS, including vulnerabilities and mitigation strategies, as well as facility managers' understanding and practice.

The following is a discussion of the security issues associated with IBMS in the modern built environment. One of the more significant outcomes of the research project is *Intelligent Building Management Systems: Guidance for Protecting Organizations*. This guidance document was developed to be a consultation tool to aid the decision making of security and facility managers, as well as provide guidance to protect a building against an array of threats and risks.

EXPLAINING IBMS

The scale of IBMS varies, from a small automated home heating system to a large and complex high-rise intelligent building, which centrally automates all functions including HVAC, lighting, elevators, audio-visual, security, and life safety systems, along with maintenance, administrative, and business functions.

With the advent of the Internet of Things (IoT), and its connectivity of all things electronic such as smartphones, vehicles, cashless vending, and more, IBMS will continue to expand into more diverse areas of everyday life. In other words, when you drive towards your building, the IoT will facilitate automatically opening the garage door as you arrive and allow your phone to open doors and turn on the building's lighting and heating.

The connectivity, automation, and control of the built environment with IBMS is achieved through a standardized technical architecture. This architecture is based on three defined component levels—management, automation, and field device.

The management level is the interface where a manager facilitates the day-to-day management of IBMS. The automation level is the core of IBMS and provides the primary automation and control devices, with controllers connected via a dedicated data network. The automation level implements defined rules set at the management level. The field device level includes the physical input sensors and output activators connected to the plant and equipment to monitor and control the built environment.

Security risks. The fact that many IBMS devices are linked through a common communications protocol introduces security risks. These consequences can be divided into categories of loss, denial, and manipulation. All of these potential hazards threaten the organization's ability to maintain occupancy, manage operations, and protect data. Such risks can result in threats to life safety, as well as major financial loss and reputational damage.

When IBMS are compromised, consequences may range from denial of service attacks to manipulation of building systems. For example, turning HVAC off is denial of control that may be uncomfortable for the building occupants as the temperature changes, but also has the potential to shut down computer network servers when they overheat.

Vulnerabilities within IBMS vary significantly, ranging from physical access to a field-level device to a highly technical remote cyberattack. Unauthorized access to an automation level controller may allow an attacker to manipulate local control of field devices or launch a cyberattack on the automation network. This attack may allow the actor to map out how the building is used, alter the automation and control programs to unlock doors and isolate alarms, and further access the network covertly.

Though IBMS attacks are rarely publicly disclosed, there are a number of notable examples. The Target breach of 2013, for instance, compromised more than 41 million payment card users when a hacker stole an internal network access credential from a third-party HVAC maintainer. In Finland, a denial of service attack on a company's network shut down the heating in two buildings. Popular hacker search engines, such as Shodan, publish a list of IBMS vulnerabilities that can be easily accessed.

Failure to understand and properly respond to IBMS vulnerabilities will result in exposure to security risks. Because of their abstract nature and the fact that they are often presented in a highly technical manner, IBMS vulnerabilities can be difficult for practitioners to understand and mitigate.

PROJECT FINDINGS

While IBMS include security functionality, most IBMS are managed and operated by facility managers rather than security professionals. However, these facility operators tend to focus more on broad organizational functions and cost management, and less on security, making it pertinent that security professionals pay close attention to these vulnerabilities.

The project found that the body of IBMS security knowledge is spread across a diverse array of literature. To date, there is no single source document that security professionals can use to understand the significance of this security concern or guide their threat mitigation.

Furthermore, the project identified several important issues in the security of IBMS: professional responsibility and the siloed effect, awareness and understanding of vulnerabilities, who the IBMS security experts are, the integration of security systems, and the lack of a common language in the security of IBMS.

Responsibility. The research found that facility professionals manage and operate IBMS, with 36 percent of participating building owners and operators indicating they have such a responsibility.

Security professionals predominately manage and operate the functional elements of the security systems, and information technology professionals manage and operate the technical elements of networked systems, including the broader IBMS architecture.

In contrast, security professionals predominately manage and operate the functional elements of the security systems, and information technology professionals manage and operate the technical elements of networked systems, including the broader IBMS architecture. Nevertheless, each profession generally focuses only on their areas of practice, resulting in silos of responsibilities.

Awareness. The project also found a significant disconnect between security and facility professionals' understanding of IBMS threats and risks and their technical knowledge of vulnerability significance. Although 75 percent of the security and facility professionals responded that they had an awareness of IBMS architecture—and half of these participants featured IBMS risks in their risk management documentation—the majority displayed a limited understanding of IBMS technology and vulnerabilities.

Both security and facility professionals rated the criticality of IBMS vulnerabilities as relatively equal in criticality.

Both security and facility professionals rated the criticality of IBMS vulnerabilities as relatively equal in criticality. Such findings support the assumption that many professionals lack technical understanding of IBMS vulnerabilities.

Expertise. Within the project, an expert IBMS technical security group emerged. Integrators—vendors, installers, or maintainers—and cybersecurity professionals displayed a more accurate understanding of IBMS vulnerabilities and their organizational significance. This group rated attacks against the automation level equipment and its network at a higher criticality. Such attacks include manual override of the controller, automation network traffic monitoring, and unauthorized access to a workstation.

Unlike the security and facility professionals, who rated vulnerabilities at about the same level, the expert group identified a significant difference between the most and least critical vulnerabilities. This demonstrates that they hold a higher level of technical comprehension that can be leveraged by organizations to achieve more robust IBMS security.

However, many integrators provide service and maintenance, rather than best-practice operational and security advice. Participants noted that advice given by integrators may be viewed as an attempt to sell their products and services, and they may not be recognized as a strategic partner providing high-level IBMS security advice.

Effective management of the security of IBMS requires that integrators or cybersecurity professionals work with the facilities and security departments. These professionals could be in-house information technology or cybersecurity professionals, or third-party contractors such as integrators.

Half of the project's participants reported that IBMS integrated into their security systems, which can put these systems at increased risk. The type of security systems used varied widely among respondents. The study also showed a discrepancy between security and facility professionals' understanding of security risks and jurisdictional responsibilities.

Language. The project found that the IBMS term "integration" is not widely understood and remains broad and undefined, with various interpretations of meaning depending on a person's occupational role.

Consequently, there is a lack of understanding and clarity of language with IBMS terms and practices. Differences in the security and facility professionals' idea of what integration means shows a cultural difference between the perspectives of IBMS. This discrepancy of language can result in a failure to address vulnerabilities to system integrity.

THE IBMS GUIDANCE

To overcome the security obstacles to IBMS, the project developed a guidance document, Intelligent Building Management

Systems: Guidance for *Protecting Organizations*. This document provides a first-generation publication for all relevant professionals to address the many and changing IBMS threats and risks, as well as the organization's ability to maintain occupancy and operations. The guidance will not only aid decision making in IBMS protection, but will help to develop a common language between IBMS stakeholders.

The guidance directs the reader to identify the organization's criticality, or impact level, if exposed to an IBMS-related event. Criticalities are ranked, using a matrix, across one or many categories such as operations, finance, safety, regulatory, information, or occupancy.

Security questions. Following are hierarchical, criticality-based IBMS security questions that are addressed. These security questions are divided into five levels of criticality that align to the criticality matrix, from low to critical. Responding to these questions facilitates either demonstrated compliance or the need to ask relevant professionals further questions.

The security questions are divided into subsections, comprising management, security risk management, personnel security, physical security, cybersecurity, incident response, continuity planning, and maintenance. A typical low level 1 security question is "Do you have a written and endorsed Security Policy?" In contrast, a critical level 5 security question asks "Do you undertake a IBMS specific threat assessment?" In all, there are 136 security questions, divided into impact levels from low to critical.

Looking ahead. Intelligent building management systems are becoming embedded into new buildings for many reasons, including the drive for greater operational efficiency and the need to meet increasing regulation. All building devices and equipment are likely to be converged with IBMS at some level of automation, including security systems.

For security professionals to have an awareness and be relevant in the modern organization, they must possess a professional level of IBMS understanding. To raise awareness and provide guidance, Intelligent Building Management Systems: Guidance for Protecting Organizations provides both the security and facility professional with the aggregated information they need to address IBMS threats and risks. Familiarizing themselves with the results of the research project will help security practitioners work alongside other personnel to provide effective security to their facilities. ◪

DAVE BROOKS, PHD, MSC, BSC IS THE POST GRADUATE SECURITY SCIENCE COORDINATOR AT EDITH COWAN UNIVERSITY IN WESTERN AUSTRALIA. HE IS THE ASIS INTERNATIONAL WESTERN AUSTRALIA CHAPTER 226 TREASURER AND MEMBER OF THE CHAPTER'S EXECUTIVE COMMITTEE. MICHAEL COOLE, PHD, MSC, BSC IS THE SECURITY SCIENCE COURSE COORDINATOR AT EDITH COWAN UNIVERSITY IN WESTERN AUSTRALIA. HE IS A MEMBER OF THE ASIS INTERNATIONAL FOUNDATION RESEARCH COUNCIL.

SECURITY
MANAGEMENT

Security From Lobby to Ledge

A $500 million renovation is set to revitalize Chicago's Willis Tower as a tourist destination, a retail hub, and one of the largest office spaces in the world—all protected by a comprehensive security program.

On the ledge nothing but a glass floor separates you from 1,353 feet of air and the pavement below. The Ledge is a glass box that extends 4.3 feet from Willis Tower, allowing 1.7 million visitors to test their nerve and experience the views from the second tallest building in the Western Hemisphere.

Willis Tower (formerly Sears Tower) was the tallest building in the world when it was originally constructed in 1970. While tourists come for exhilarating 1,800-feet-per-minute, ear-popping elevator rides to the top and the expansive views of the Chicago skyline, 15,000 people come to the iconic building every day to work. They represent the top 100 firms in Chicago, including an international airline, law firms, trading companies, and high-tech entities.

While many marvel at how a glass floor can sustain a constant flow of visitors, those familiar with the structure know that The Ledge and the tower are protected by more than plates of glass. They are protected by a complex security management program, rated as best-in-class by the U.S. Department of Homeland Security, and encompassing physical, operational, and technical systems. And now, the skyscraper is engaged in a $500 million transformation that will result in significant impacts on its operations and security, from The Ledge to the lobby.

THE FOUNDATION

Willis Tower is one of the largest office buildings in the world, encompassing more than 4.5 million square feet of space—the equivalent of 78 football fields. Today, the tower welcomes approximately 20,000 tenant employees, tourists, business visitors, building employees, and deliveries each day.

The tower relies on a combined command center of building engineers and security staff to monitor the building's video surveillance systems, access control alarms, intrusion detection, and continuous fire and life safety systems, along with the tower's heating and cooling, water, and electrical systems.

The command center staff can pinpoint the exact temperature and electricity used for each floor and track the movement and destination of its numerous elevators. The building was the first to have automatic sprinklers cover every square foot of the property, and its advanced smoke detectors can zero in on the source of smoke and alert the command center to activate the exhaust system.

Security practitioners know that tracking dynamic security conditions is infinitely more complex than detecting smoke, and that is certainly the case here. The building management firm at Willis Tower, EQ Office (EQ), relies on security staff members to monitor the building in the command center, patrol the public areas, and man stationary posts at the loading docks, common spaces, tourist areas, and throughout the building at all hours.

The program encompasses a detailed security management approach to emergency planning and response, technology and personnel vetting, monitoring of packages, and evacuations. This is in addition to security and life safety training for the security team and tenants, coordination with all levels of law enforcement, and extensive documentation.

Training is paramount, especially since a major focus for the renovation is customer service. With so many diverse visitors, areas for misinterpretation are continually present and must be carefully addressed. For instance, how does a security officer on patrol tell the difference between tourists taking photos inside the building and potentially malicious reconnaissance? To address these and several other potential scenarios, in 2018 the security and life safety team trained for nearly 6,000 hours on topics encompassing active shooter, emergency operations, customer service, building navigation, and control room operations.

THE EXPANSION

"Catalog" is the soon-to-be-completed five-story, 300,000-square-foot dining, retail, and entertainment space at the base of Willis Tower. The name is a historical nod to its original developer and owner, Sears Roebuck, and its famous printed catalog. From a security perspective, this project means more square footage to monitor and patrol, more members of the public entering the space, and more media attention.

Currently, the tower's publicly accessible retail operations are limited to the main lobby. However, the renovation plans for Catalog entail a major expansion in retail operations, including creating multistory restaurants, apparel shops, fast food eateries, coffee shops, retail venues, and a public roof deck. The overall goal is to enhance the service available at the facility and increase pedestrian access to the building beyond the typical 8 a.m.–5 p.m. business hours. The increased traffic and expanded business hours are expected to create new security challenges for the facility.

The overall goal is to enhance the service available at the facility and increase pedestrian access to the building beyond the typical 8 a.m.–5 p.m. business hours.

EQ recognized this early and committed to ensuring security was at the forefront of these plans, while maintaining the building's Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act designation. The SAFETY Act is part of the Homeland Security Act of 2002 and is administered by the Office of SAFETY Act Implementation (OSAI) at the DHS Science and Technology Directorate.

The program was created to address private sector liability concerns and the lack of incentive to implement or develop anti-terrorism technology. It offers liability protections for providers of Qualified Anti-Terrorism Technologies to encourage the development and deployment of these products. Under EQ's management, the building has held its SAFETY Act designation for the Willis Tower Security and Life Safety Services since 2013. The DHS recertified the tower's SAFETY Act Designation in 2018. To maintain the designation, Willis Tower must report any planned changes to its program for review by DHS authorities.

The effort to maintain the vertical village's high-caliber security program and SAFETY Act designation included a partnership between EQ and Guidepost Solutions, LLC, a security and technology consulting firm. Together, they assessed how the plans might impact onsite security and oversaw installation and testing of the security systems during the renovation.

It's important for security to be involved in renovation and construction plans from the beginning; however, security is often the last discipline brought to the design table for input. This can result in poorly considered security solutions, lack of proper balancing of risks and controls, and a disregard for how the building will function and provide protection. In this case, EQ Office took the opposite approach by trusting the leadership of its security director and team.

This level of commitment to security is not new for EQ. Immediately after the 9/11 attacks, the Willis Tower team started preparing for the worst by consulting with safety and security experts to unify around the principle of providing safe, inviting spaces for employees and visitors. This approach to security has been adopted across EQ's 80 locations, which comprise 40 million square feet of Class A office space throughout the United States.

Gary Michon, general manager of Willis Tower, says that "the key to this project was to bring Guidepost in early, so that we could properly plan and execute the expansion of our security systems to properly monitor and control access to more than 20,000 tenants and visitors who enter the building each day. Throughout the entire planning process, we focused on the customer access and their experience with the new technologies that are being introduced to the building and Catalog."

The Willis Tower redevelopment project is a mammoth undertaking because the base floor of the building anchors high-rise towers and defines the pedestrian experience on the street level. EQ and Guidepost Solutions worked collaboratively to develop the security program with the focus on the tenant and guest experience. The project includes major enhancements to public areas across multiple floors, a rooftop space on the fourth level, all new lobbies and entrances, and new physical security solutions, such as the use of barriers; segregation of office building tenant, visitor, and public areas; barrier turnstiles that can handle 70,000-plus transactions per day; screening rooms for visitors; duress alarms; surveillance cameras; card readers; integrating elevator destination dispatch systems; and implementing a new visitor management system.

One of the significant challenges of the renovation is the increased foot traffic through the lobby, so the improved screening lanes and organized access management are imperative. The new security measures are intended to provide tenants with a user-friendly and comfortable workspace, business visitors with an efficient method to reach tenant floors, and visitors with a welcoming environment to explore retail stores, restaurants, and entertainment venues in the Chicago landmark.

Willis Tower is steadfast in maintaining its high-quality security program and ensuring the redevelopment project does not interfere with its site security posture commensurate with other similar tourist destinations. Indeed, the EQ team used the challenges presented during this project as an opportunity to provide needed security technology enhancements, focusing on replacing obsolete technology with devices capable of integrating with current systems. In addition to upgrading its surveillance cameras, Willis Tower is in the process of establishing a gunshot detection system that will monitor common areas, alert staff to emergency situations, and—via integration with the elevator systems—direct elevators away from the identified danger.

Another important element of the security strategy is the overall tenant–guest experience. Tenants of the building invite more than 350,000 visitors a year to their offices, and each visitor must register and go through x-ray and magnetometer screening equipment similar to Transportation Security Administration lines at the airport.

EQ and Guidepost Solutions developed a way to streamline this process by harnessing technology that can support multiple methods of checking in visitors. Visitors can check in by using an email or mobile pass on a smartphone, at a manned lobby desk, through a mobile concierge officer, or self-check-in at multiple kiosks.

This flexibility allows the security team to scale up their personnel levels during peak visitor times, quelling lines while offering a high-quality guest experience. Willis Tower is reaching out to tenants to share information on the new visitor management system to prepare the tenants for the influx in traffic to the tower.

In addition, the new system adds layers of security and authentication by integrating driver's license readers into the self-service kiosks and using license plate reader technology for dock access.

This flexibility allows the security team to scale up their personnel levels during peak visitor times, quelling lines while offering a high-quality guest experience.

To further enhance the tenant experience, EQ and Guidepost Solutions are implementing IDEMIA's MorphoWave biometric technology, integrated into 26 new Automatic Systems Slimlane turnstiles for tenants who opt in to the building's amenity program. The biometric technology provides frictionless access control and allows authorized tenants to wave their hand above the device's touchless sensors for access, forgoing the need to present a credential. The turnstiles also include technology for phone-based mobile credentials and regular card readers to maximize flexibility in how tenants experience processing through the turnstiles each day.

For the much-anticipated common space, EQ sought an array of security measures to provide clear situational awareness. The common areas within the main lobbies on Franklin Street, Jackson Boulevard, and Wacker Drive will have surveillance cameras strategically located to observe and record activity.

Other measures include providing architecturally designed full-height partitions and solid doors to protect back-of-house operations and elevator access from common areas, while card readers and alarms will control access throughout. EQ installed an additional local security operations room near the new common space to focus on monitoring the public areas during normal business hours, as opposed to the entire complex.

Willis Tower is stepping away from a traditional security strategy, instead facilitating a neighborhood approach to serve as the cornerstone for the entire project by providing clear divisions between screened and unscreened individuals and deliveries. This method focuses on reinforcing a highly active, community-based environment that encourages professional networking.

Under this approach, non-screened individuals can access the common levels, but multiple layers of controls manage access to tenant spaces and allow for enhanced monitoring capabilities via analytics. The purpose is to reduce the expense of monitoring, a task with a limited return. The technology in place detects changes in the environment and alerts security staff to unusual activity, freeing up personnel and resources to monitor areas with fewer controls, such as the lobbies or common areas.

For example, instead of requiring constant monitoring of camera surveillance and guard posts, staff can use the sensors to identify any abnormal activity. This change enables them to provide greater coverage while simultaneously decreasing screen time and improving response capabilities.

Overall, major renovations can create considerable security concerns, particularly when the public area footprint of the site is expanding, a common trend in Chicago and commercial real estate. Such projects, however, also offer opportunities to evaluate the current security program in place, determine areas for improvement, and provide a means to consider needed security enhancements—and sooner in the process is always better.

It is essential to ensure leadership supports the process early, security expertise is sought and included in the design phase, and the transition process is managed to identify areas of potential risk while maintaining a valuable security certification. The key is constant communication and transparency.

KEITH KAMBIC, CPP, IS THE SENIOR DIRECTOR OF SECURITY AND LIFE SAFETY FOR WILLIS TOWER. HE IS A MEMBER OF THE ASIS COMMERCIAL REAL ESTATE COUNCIL AND BUILDING OWNERS AND MANAGERS ASSOCIATION OF CHICAGO EMERGENCY PREPAREDNESS COMMITTEE. EDWARD BATCHELOR, PSP, BRINGS MORE THAN 15 YEARS OF PHYSICAL, TECHNICAL, AND OPERATIONAL SECURITY DESIGN AND CONSULTING EXPERIENCE TO HIS ROLE AS GUIDEPOST SOLUTIONS' REGIONAL DIRECTOR IN CHICAGO. ANGELA J. OSBORNE, PCI, IS A REGIONAL DIRECTOR FOR GUIDEPOST SOLUTIONS BASED IN WASHINGTON, D.C., SERVING ON THE ASIS COMMISSION ON STANDARDS & GUIDELINES AND ADVISOR TO THE YOUNG PROFESSIONALS COUNCIL.

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.