SECURITY
MANAGEMENT

Fostering a Security Awareness Culture

This collection of articles from the security profession's premier publication discuss the skills and techniques security leaders can use to ensure security is embedded into the culture of their organizations.

Powered by

ASIS INTERNATIONAL

Advancing Security Worldwide®

SECURITY MANAGEMENT

Security in Context

Robust security technology, guarding programs, and threat assessment programs can fall flat when implemented without one essential element—contextual intelligence.

By Diana M. Concannon and Michael Center

You are the recently appointed chief security officer of a major multinational corporation. You have more than 20 years of upper-level law enforcement experience in your home country, and your first major project is a review of the company's Tokyo facility. A team of experts and vendors has been put together to review the threats specific to the locale and the vulnerabilities of the facility.

Months of analysis and review have gone into the project. Additional time has been spent installing perimeter upgrades, baggage and parcel screening technology, and magnetometers. Dedicated and guarded employee parking areas have been constructed and operationalized. More than $250,000 has been invested in hardware alone.

Finally, the project is complete. You have contracted a local security professional to conduct a red team active review of the installation to measure its effectiveness. No more than 15 minutes after the start of the test, the expert calls you from

the executive conference room, having bypassed the entire physical security system you worked so hard to put in place.

When asked how this was achieved, the penetration tester replies: "I copied the company's logo from the Web, used a color printer and laminating paper to make a simulation of a badge, and told the front desk that I had flown in from U.S. corporate for an emergency audit meeting. I said that the CEO demanded that I start immediately, and I do not know why my ID card does not work. They let me right in and led me to the conference room."

In implementing the sophisticated physical security measures, the CSO neglected to consider one thing: the culture of the workers, who were reticent to confront an individual who claimed to be in a position of authority.

CULTURE AND CONTEXTUAL INTELLIGENCE

Culture is one of many elements that today's security professionals must consider to successfully navigate redefined boundaries related to geography and diversity, and even in relation to education, experience, and expertise.

Incorporating the impact of culture in decision making exemplifies the application of contextual intelligence—a concept used for decades in the management and sports sectors—to contemporary security practices.

Context is the background against which an event takes place; it makes information meaningful. Intelligence about context enhances situational awareness and enables more relevant, efficient, and practical decisions.

A great deal of attention has been given to affective or emotional intelligence, which focuses on the realm of moods and feelings. It was originally formulated by psychologists Peter Salovey and John Mayer, and popularized by psychologist and science writer Daniel Goleman. Emotional intelligence focuses on self-awareness, self-control, and empathy.

Improving one's understanding of emotional intelligence is often promoted as a necessary skill set for improving people management and job performance. (For more information, see "Harnessing the Power of Emotions," Security Management, September 2015.)

Contextual intelligence, coined in 1984 by Yale University psychologist Robert Sternberg, is a cognitive process that involves thought, understanding, and perception. Contextual intelligence prioritizes the environment, relying upon three primary processes to optimize decision making: adapting to the environment to meet our objectives; shaping the environment to meet our objectives; or selecting to abandon a project altogether.

Different industries have employed various methodologies to determine whether it's best to adapt, shape, or abandon endeavors.

In the security sector, we recommend a simple framework, encapsulated by the mnemonic COPE—culture, organizational values, politics, and environment—to apply contextual intelligence to enhance decision making at the executive and managerial levels and on the front lines.

CONTEXTUAL INTELLIGENCE IN ACTION

Contextual intelligence is pragmatic and allows for nuancing the all-hazards approach to more effectively prepare and respond to security risks. Incorporating contextual intelligence into a proven threat assessment model enhances its efficacy.

Culture, the first element of the COPE framework, can be defined as the customary beliefs, social norms, and racial, religious, or social group characteristics shared by people in a place or during a time.

In the Tokyo security example above, an understanding of the deferential culture of the employees responsible

for the reception areas might have mitigated the security breach during the penetration test. In response, the organization could have adapted the environment to eliminate the need for staffed entrances or shaped the environment through targeted training of frontline security.

In his primer for army personnel on the front lines in Iraq and Afghanistan, U.S. Lieutenant Colonel William D. Wunderle offered the example of U.S. troops forcing the heads of Iraqis to the ground during arrests—an act which violates Islamic religious norms of not allowing the head to touch the ground except in prayer. Behaviors that offend cultural norms can

Culture, the first element of the COPE framework, can be defined as the customary beliefs, social norms, and racial, religious, or social group characteristics shared by people in a place or during a time.

undermine core security missions; in the case of the global war on terrorism, offending detainees and the populace who witnessed the arrests threatened to undermine the mission of bringing stability to the Middle East, Wunderle said.

However, research on cultural competence across disciplines has found that knowledge of norms and customs is but one element to being successful. The capacity to assess one's own cultural biases, to value diversity and manage differences, and to accommodate another's worldview are also key. The deeper understanding of another's perspective—derived from cultural competence—enhances the ability to predict behavior.

PRIORITIES AND VALUES

The second element of the COPE mnemonic, organizational values, seeks to ensure that any security plan, decision,

or response aligns with institutional priorities. Consistent with the enterprise security risk management (ESRM) approach, the consideration of organizational values as a facet of contextual intelligence supports transcending security silos between people, assets, and processes, and between security and business outcomes.

Efforts to replace the so-called school-to-prison pipeline phenomenon in the United States with alternative classroom management approaches exemplify consideration of organizational values in action.

Highly publicized active assailant incidents in public and private schools in the past decade have given rise to two dynamics that have contributed to higher arrests of schoolchildren: an increase in the number of school resource officers (SROs), and a decrease in tolerance levels for disruptive classroom behavior, which is often regarded as a high indicator of risk for violence.

An increasing number of institutions are seeking security solutions that are more congruent with their educational values. Alternatives—such as restorative justice, which emphasizes accountability, peer learning, and meditation in response to unacceptable behavior—are being explored.

SROs can be instrumental in these efforts, adapting their expertise in de-escalation, risk communication, and behavioral threat assessment to support safety without criminalization. Considering factors such as age, developmental level, and social status within the school environment can contextualize benign behaviors that might otherwise be perceived as threatening or insubordinate.

POLITICAL CONTEXT AND ENVIRONMENT

Politics—the third element in the contextual intelligence mnemonic—is defined here as the larger context in which a situation is occurring and the specific influences that may need to be evaluated.

Consider events in China in 2008. After an earthquake destroyed 67 percent of the habitats of China's beloved panda bears, a type of panda mania set in worldwide. Pandas are typically popular—researchers suggest pandas activate regions in human brains like those triggered by human infants (recall their snub noses, wide cheeks, and toddling gaits)—but the events of 2007 sparked a surge in merchandising.

Against this context, it was perhaps not completely unsurprising when a 20-year-old student visited Qixing Park in Guilin, China, and scaled a 6.5-foot wall to enter the panda enclosure. He was repeatedly bitten by Yang Yang, one of the zoo's pandas, before being rescued by zookeepers. The student subsequently claimed that he "just wanted to cuddle" the panda, according to the official Xinhua News Agency.

The larger political context at the time—in this case, a heightened interest in pandas—might have suggested that relying on a 6.5-foot barrier and the common sense of visitors might not be adequate to achieve a primary security objective of maintaining separation between humans and the very popular pandas. The environment and its security might have benefited from being shaped to match the larger political context.

In contrast, environmental context refers to local events and influences.

The impact of environment on security during the current COVID-19 pandemic is exemplified by an early effort by a southern California public–private partnership. In March 2020, the collaborative unveiled plans to slow the virus's spread by treating potentially coronavirus-positive homeless patients at vacant hotels. One of the chosen facilities was proximate to a community of 18,000, many of whom were in the high-risk 65 and older age group.

The result was a series of protests, online petitions, and dissemination of misinformation. A plan that worked perfectly across multiple environments was not adapted to the local conditions of an older community and resulted in civil disobedience and multiple security risks.

In contrast, a community health center—mindful that its surrounding neighborhood generally responded to change with anxiety and unrest—opted to test potential COVID-19 patients discreetly; rather than erecting a parking lot tent, patients were tested in their cars. The healthcare response was adapted based upon the environmental context.

CAN CONTEXTUAL INTELLIGENCE BE TAUGHT?

Traditionally, it has been believed that contextual intelligence could not be taught directly: You either had it, or you didn't. But research in various areas—most notably business and sports psychology—has helped debunk this myth.

As industry globalized, business schools recognized the necessity of ensuring that future industry leaders understood contextual intelligence if businesses were to succeed in emerging markets. Tarun Khanna, economic strategist and Harvard Business School professor, used the example of a cement factory.

He pointed out that although the process for making cement is consistent across factories, the context in which a factory is embedded can influence everything from whether corrupt suppliers adulterate mixtures, to whether workers are unionized, to the way in which the final product is sold locally. The company seeking to relocate a plant to a location that might appear to offer greater return-on-investment potential must understand the impact of the contexts in which the business will operate.

Over time, the incorporation of contextual intelligence

on business curricula and, subsequently, practices have allowed for interesting innovations. Popularized by sociologist Roland Robertson, "glocalization" can be viewed as the adaptation and shaping of contextual intelligence in action. It has resulted, for example, in one's ability to purchase both a Big Mac and Seaweed Shake Shake Fries when at a McDonald's in Hong Kong.

Likewise, sports psychology teaches its practitioners to intentionally consider the context in which they are working with athletes—the culture of the team and the sport, the values of the league, politics surrounding sponsorship, and the influence of local fans—to support maximum individual performance in their clients.

TEACHING COPE IN SECURITY

Contextual intelligence can also be taught and learned at all levels of the security team by integrating COPE factor analysis into relevant decision-making processes.

On the front lines, this occurs through COPE inclusion in various drills, thought experiments, and operational templates. It involves movement beyond standard—and frequently superficial—training in cultural competence to training that has greater relevance, depth, and impact.

The use of case studies, for example, allows security professionals to develop knowledge of cultural nuance and test their ability to predict behavior based upon this knowledge. Then they can compare their predictions against real world results.

For example, are frontline security professionals for a hypothetical Malaysian e-commerce company able to detect and prioritize potentially significant nuances related through case studies: What is different today from yesterday? Are children playing in the neighborhood as normal?

Are they suddenly gone? Are there new faces in the area? Have local radio stations increased negative mentioning of internationals? Has the village matriarch invited you to take tea, as usual? Or, are there more males and fewer females present than normal?

What does the subtle presence of the cultural normal or its absence potentially mean? Conversely, what does the presence or absence of that which is culturally incongruent signify? What could these subtle changes signal?

This approach can also uncover implicit biases that most of us hold—and about which we are typically unaware. In at least some areas, unrecognized biases can impede successful decision making.

A bias, for example, that men are more lethal than women can create a vulnerability if an organization dismisses early warning signs from a high-risk female.

MANAGING WITH COPE

On the managerial level, the inclusion of COPE factors assists in professionalizing the workforce, connecting members of the security team more closely with organizational missions, and providing a forum to review the often shifting macro- and micro-influences that affect the provision of services in various industries.

COPE may cause managers of security at a large metropolitan hospital, for example, to shift a drill's focus from active assailants to workplace domestic violence or a pandemic based upon a sensitivity to the hospital system's culture and organizational values of supporting the physical and psychological safety of its workforce, coupled with an ongoing analysis of threats in large hospital systems regionally, as well as the emergency department specifically.

At the executive level, COPE provides a framework for both considering and informing critical institutional deci-

sion making by casting security intelligence in the broader themes that are vitally important to an organization's ability to survive, particularly during times of change or complexity. Using the COPE framework, for example, may inform recommendations to abandon reallocating resources from current security efforts—which can be demonstrated to align with culture, organizational values, and current political and environmental events—over a security proposal that has limited or no utility to the institution's larger goals.

CAN CONTEXTUAL INTELLIGENCE BE ASSESSED?

Assessing the contextual intelligence of security job applicants can be achieved through case studies that evaluate contextual sensitivity. Industry-specific hypotheticals that require the candidate to articulate the factors they would consider when engaging in decision making can assess contextual intelligence.

Psychologist Robert Sternberg offered the following example of operationalized contextual intelligence in a workplace setting.

An employee loved his work, coworkers, and where he lived, but hated his boss. The employee was contacted by a recruiter who had heard of his dissatisfaction and offered him a position with considerably more pay and responsibility at a company in a nearby city. The employee declined the position and instead gave the recruiter his boss's name. His boss took the job.

Sternberg's example demonstrates each of the factors suggested by COPE—cultural consideration, an evaluation of the role of organizational values, politics, and the environment—to arrive at a pragmatic and creative solution.

To see how contextual intelligence can be leveraged in a security setting, consider the following anecdote.

Doctors and mental health workers at a maximum-security penitentiary are threatening to strike, claiming safety concerns stemming from a lack of rapid response by correctional officers to panic calls. They cite two staff who were badly injured over the prior three-month period. Correctional officers, in response, report that the majority of calls by workers are false—either made by accident or never received. A strike would threaten the facility's ability to provide needed care to inmates and obtain a coveted accreditation status, and it could generate negative publicity. What factors would you consider when developing a security solution to this situation, and what potential resolutions do you envision?

Applying the COPE framework supports an evaluation of the security candidate's response. Does the candidate consider the potential cultural differences between medical and correctional staff and offer thoughts on ways to bridge any possible divide? Does the proposed response include an investigation of the institution's values and priorities, perhaps identified through how it managed the incidents with the injured workers? What are the political ramifications of obtaining—or losing—the specialty accreditation? And, have there been recent local or sector-specific news events that render the institution particularly vulnerable to negative publicity at this time?

A contextually intelligent applicant will likely respond to such a scenario in a way that moves beyond a limited focus on modifying equipment (a simple abandonment of the current hardware) to a more sophisticated plan that includes adapting to and/or shaping the current environment. For instance, the development of scaled responses based upon inmate risk levels, with the establishment of special joint healthcare–correctional officer deployment teams for the highest risk populations.

THE CONTEXTUALLY INTELLIGENT SECURITY TEAM

Contextual intelligence and the COPE framework support the professional development of individual security personnel—whether in the C-suite, at the managerial level, or on the front lines—through the enhancement of decision-making skills. Training members at all levels of the security workforce also supports the establishment of a consistent problem-solving approach that can unify diverse members of a security team, improving the ability to coordinate and collaborate across roles.

In this way, a shared commitment to considering culture, organizational values, politics, and environment to inform whether to adapt, shape, or abandon situations promotes the contextually intelligent security team's capacity to successfully meet today's complex security challenges.

DR. DIANA M. CONCANNON IS A FORENSIC PSYCHOLOGIST, ASSOCIATE PROVOST AT ALLIANT INTERNATIONAL UNIVERSITY, AND DEAN OF THE CALIFORNIA SCHOOL OF FORENSIC STUDIES. SHE IS SPECIAL ADVISER OF ASIS INTERNATIONAL'S PROFESSIONAL DEVELOPMENT AND SCHOOL SAFETY AND SECURITY COUNCILS. MICHAEL CENTER IS A REGIONAL SECURITY ADVISOR FOR THE UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY BASED IN BRUSSELS, BELGIUM. HE IS CHAIR OF THE ASIS PROFESSIONAL DEVELOPMENT COUNCIL AND CO-VICE CHAIR FOR SUBJECT MATTER EXPERTISE OF THE GLOBAL TERRORISM, POLITICAL INSTABILITY, AND INTERNATIONAL CRIME COUNCIL.

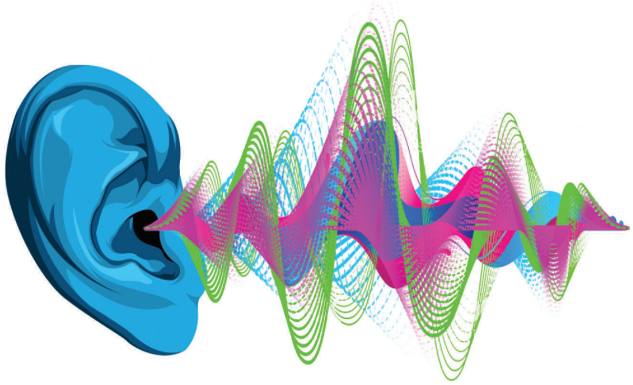
THE VIEWS EXPRESSED IN THIS ARTICLE ARE THE AUTHORS' OWN AND ARE NOT REFLECTIVE OF THEIR ORGANIZATIONS.

SECURITY MANAGEMENT

Watch Your Language

Managers are often judged on how well they communicate. Leader language is clear and tight, informed by the big picture, and it conveys an "I'm listening" message.

By Eugene Ferraro, CPP, PCI



Who would the CEO of your organization most likely invite to a round of golf: the CFO or you? The answer to such a question would be revealing—and it shows a great deal about security professionals and how they are viewed by their contemporaries.

It has become a truism that in order to maximize effectiveness, one must have a seat at the table in the C-suite. And communication skills will likely play a paramount role in whether or not the organization's ranking security professional ultimately earns that seat.

Business executives realize that, like it or not, their usefulness to others is regularly assessed and measured. That continual evaluation is reality. Security professionals who aspire to earn a place in the C-suite should realize that this situation is their reality, too.

Given this, security professionals who regularly speak and write in the language and style of the military and law enforcement run the risk of being valued differently

from those who have MBAs and can communicate in the language of a modern business executive. Regardless of the ultimate value of their contributions, if security professionals communicate more like law enforcement officers than business executives, they will eventually be treated as such, and be compensated accordingly.

Much has been written on the broad topic of management and leadership development. But there is less guidance on the more specific area of executive communication, and the importance of these skills to the leader's success. This is unfortunate, because in the workplace the language and presentation of an idea can be nearly as telling as the idea itself. Sometimes, a staffer will take his or her cues from this language when trying to evaluate the significance of the idea itself. A sound idea, poorly expressed, can be unfairly dismissed.

GETTING ON THE SAME PAGE

First and foremost, security professionals must recognize that one's professional success is not just the product of doing a job well. It also depends on the ability to effectively communicate and adapt.

A manager cannot succeed by resting on the laurels of past accomplishments. However justifiably proud a security professional is about past accomplishments and successes, he or she should realize that current customers—whether internal or external—were not necessarily the direct beneficiaries of those past triumphs. In order to provide value, professionals must be able to continually and effectively communicate with colleagues and customers whose needs and expectations are in the present.

Consider that the three most used business language phrases in 2018 were "we're on the same page," "action plan," and "game changer," according to linguists.

These terms are still heard frequently in workplaces, including security departments. Why might this be?

These phrases imply the need for action. When used in conversation, they communicate recognition of the increased productivity that will likely result when people get on the same page and agree to pursue a well-considered action plan. When executed properly, the resultant output is often a game changer. The phrases themselves may be getting a bit shopworn, but they still reflect the importance of teamwork and effort.

Considering similar questions in advance—including how security can contribute to these business goals—helps a security professional show that he or she is on the same page as the executive.

In addition, "getting on the same page" also has relevance when considering effective executive communication. To be on the same page as a C-suite executive often requires the ability to adopt a higher-level perspective.

For example, a manager is briefing the CEO about a security-related operational development. Before the conversation starts, the security professional should consider how the situation might look from the CEO's perspective: How might this security development impact the company as a whole? Is there any long-term significance for the company? Can this development somehow help enable overall business growth?

Considering similar questions in advance—including how security can contribute to these business goals—helps a security professional show that he or she is on the same page as the executive. This preparedness and consider-

ation helps establish the manager's bona fides as a voice worth listening to.

Communicating big picture impact may also assist a manager with another key communication component: getting to the point. Most C-suite executives have multiple demands on their time, so a security briefing that seems to go on and on may not be well received. Big picture summaries serve as an effective way to end the communication: "The bottom line here is that this situation could be pervasive enough to impact…" Proposing solutions can effectively underline the conversation, but here the manager must be careful. In some cases, a solution may not be apparent, and it is dicey to suggest one that has a high possibility of failure.

Nonetheless, it is advisable for the manager to prepare for possible questions. For example, the manager can think about what might be unclear, especially to a non-security specialist, and have a thumbnail explanation at the ready. This can help professionals avoid getting bogged down with unnecessary detail as they struggle to explain concepts. If a manager is not exactly sure what the root of the confusion is, clarifying questions (e.g. "So what you want to know is how the funding aspect works?") can help, so the manager does not waste executives' time providing the wrong information.

In conjunction with preparing for questions, it may also be helpful for professionals to keep any arguments or proposals they are making as tight as possible. Avoid exaggeration or alarmism when discussing a problem. Double-checking statistics and spending time on the logical flow of arguments are good ways to do this. This can take additional preparation or a rehearsal, but it is usually worthwhile.

KNOW YOUR AUDIENCE

For many security professionals, the majority of communications involves staff and coworkers, as opposed to C-suite executives. In most workplaces, employees vary in age, but recently a relevant trend has emerged. Millennials—people born between 1981 and 1996, currently aged 24 to 39, according to the Pew Research Center—are now the largest generation in the U.S. labor force.

By dint of this statistic alone, it is likely that a sizable portion of most companies' employees will be in this age range. And a tried-and-true rule for communication is to know your audience. Social change and dynamics are shifting rapidly in many workplaces today, and clear and appropriate expression is more important than ever. If a company's workforce is majority millennial, it behooves

Younger employees' interest in seeking recognition suggests that professionals should regularly recognize them in their communications.

a manager to know some of this age group's common qualities and attributes, so that communication style and content can be shaped for maximum effectiveness.

Those who study generational differences and behavioral patterns say that many millennials bring vitality and passion into the workplace, plus a strong desire to be heard. Many millennials also tend to openly seek recognition, fairness, and justice, regardless of their place on the organizational chart. For them, the rigidity and dogma of the past are obstacles to progress.

Security professionals should consider what these characteristics mean in terms of communication effectiveness.

Millennials' strong interest in being heard suggests that professionals should ensure their communications solicit input and feedback. Younger employees' interest in seeking recognition suggests that professionals should regularly recognize them in their communications. And their interest in fairness and justice suggests that managers should pay attention to those factors when explaining company policies and actions.

SPEAK TO, NOT AT

While some communication methods suit certain demographics over others, some tips are universal. For example, always speak to someone, not at someone.

When verbally communicating, a manager should not attempt to either impress or suppress the other party—he or she should not try to approach the conversation as a competitive contest in which the winner wrests control from an opponent. Unfortunately, some professionals do strive for conversational control, either by piling on self-acknowledgments or actively minimizing the partner's participation.

Instead, a manager should strive to acknowledge the conversation partner's point of view. Doing so validates the other party and demonstrates the manager's interest in their input. Such an acknowledgment reflects active listening, and it communicates positive recognition. In addition, such acknowledgment may lead to further discussion of their idea. This can give a manager more insight into the idea, and ultimately he or she can respond more intelligently.

ELECTRONIC COMMUNICATION

As remote workforces expand and digital communication becomes the default, a manager should err on the side of professionalism.

When communicating electronically, avoid shouting. DO NOT USE ALL CAPS or end your message with "……..," "??????," or "!!!!!!!". The overuse of casual text abbreviations (lol, omg) should also be avoided.

Some experts recommend that, when replying to emails, a manager should always take an "executive pause" before firing back an angry reply. If the email that the manager has received is a provocative or accusatory one, the manager may want to set it aside and come back to it later, in order to send a more measured response.

Remember also that electronic communications, including text messages, are discoverable in the event of litigation. Childish or disrespectful communications can be embarrassing or worse for a security manager if he or she must later testify before a judge or magistrate.

In addition, curtail multitasking. Emailing while chatting with a coworker is not only rude, but it hinders the manager's ability to learn. Verbal communication in the workplace is a great way to exchange information. While multitasking is sometimes praised by professionals as a way to enhance productivity, it can produce misunderstandings when mixed with verbal communications.

In addition to verbal and electronic communication, be aware of body language.

Many human resources professionals and some security professionals have received training on the use and interpretation of body language. This can often be useful.

For example, experienced fact finders know that when they are being told something less than truthful during an investigatory interview, putting down their pen and notepad silently communicates disbelief of what was just said.

Looking away during a conversation demonstrates a lack of interest in what is being discussed. Managers must be mindful of these messages.

Body language offers a manager an effective way to convey openness with a clear listening stance. Giving executives and coworkers alike full and comfortable attention while speaking, without distracted gestures like fidgeting and checking the time, is a boon for effective communication. It conveys interest and respect, and it engenders confidence that the communication will be productive. It also shows that a manager leads by listening, which in the end is one of the most quietly effective leadership styles of all.

EUGENE F. FERRARO, CPP, PCI, SPHR (SENIOR PROFESSIONAL IN HR), IS A GRADUATE OF THE NAVAL JUSTICE SCHOOL AND HAS BEEN THE PROGRAM ADVISOR FOR THE PCI REVIEW COURSE FOR 12 YEARS. HE IS FOUNDER AND FORMER CEO OF THE GLOBAL COMPLIANCE AND WHISTLEBLOWER HOTLINE PROVIDER CONVERCENT, INC.

SECURITY MANAGEMENT

Where Science Meets Experiment

To avoid emotional, knee-jerk responses to tragic events, security professionals turn to research to ensure strategies are effective.

By Diana M. Concannon and Michael Center

As the interconnectedness of the world increases, increasingly complex yet similar challenges stretch across sectors and geography. Like their public safety colleagues in the military, law enforcement, and fire services, private security professionals are increasingly recognizing the need for evidence-based practices. Such methods can improve the efficiency and effectiveness of their operations, to avoid wasting limited assets and resources, and to satisfy executive demands for data-driven programs and projects while preventing the implementation of well-intentioned but ill-informed executive directives that are destined to fail.

Violent global incidents—amplified by the 24-hour media news cycle, social media, and citizen journalism—create a false sense of urgency to implement new, irrelevant, ineffective, or unnecessary initiatives in the organizations we protect.

Highly publicized events—such as stabbings in North London, kidnapped tourists, or the discovery of unexploded improvised explosive devices (IEDs)—are frequently overgeneralized to misrepresent broader security threats. Media coverage of violent incidents is often highly disproportionate to the probability that individuals or organizations will likely experience such violence firsthand.

Despite this, decision makers often attempt to address the emotional and psychological distress that ripples from tragic events through knee-jerk security responses—regardless of whether the solution in question may be ineffective or, worse, counterproductive. Lone incidents, while shocking, do not necessarily indicate trends that require changes in programs and priorities. While convincing employees, stakeholders, and ourselves not to react hastily is challenging, being armed with appropriate and objective knowledge can help.

Research serves as a valuable tool in helping security leaders fulfill their roles in creating, maintaining, and evolving security programs. Scientific insights can aid in creating effective, appropriate, and sustainable security responses—ones that are not usurped by emotionally galvanized reactions to a single event or generic, traditional security plans that do not fit the current risk landscape.

Finding or developing evidence-based practices is particularly important in relation to prevention and preparedness efforts, where security and law enforcement personnel's investigative and after-action experience does not translate as readily. Using research to confirm, supplement, or replace traditional responses to security incidents is critical in budget-based decision-making processes.

Combining science with professional experience to prevent and assess violence risk has proven more effective than reliance on either one alone. While a singular

focus on research overlooks the dynamic and contextual factors that influence risk levels, depending solely on one's professional judgment or experience narrows options to personal knowledge, experience, biases, and skill sets, which may not be the most advantageous in a situation. Nor is personal opinion a very compelling argument for securing vital assets in most resource-competitive environments.

Fortunately, there are numerous immediate, low-cost—if not free—resources available to security professionals.

THEORY INTO ACTION

Say that you are the vice president for security of a rural hospital system. The chief information officer calls you into her office to report that Human Resources has been "flooded" with calls from staff following an active shooter incident at a nearby hospital that dominated the news. A 32-year-old gunman confronted, shot, and killed his ex-fiancé, a doctor, in the parking lot. When law enforcement responded, the gunman fled into the hospital, where he killed a pharmacy intern and a law enforcement officer before killing himself.

The event echoed another highly publicized hospital-based shooting that occurred several months prior, heightening hospital staff's anxiety—despite the fact that this incident was later determined to be a murder–suicide; the shooter was a 71-year-old male who, distraught over the illness that plagued his 70-year-old patient wife, murdered his spouse before killing himself in the hospital.

Although the CIO appreciates your efforts to standardize and elevate the hospital's emergency operations plan over the past year, the feedback she received indicates that workers feel more prepared to deal with a pandemic outbreak than violence, "particularly if it is someone's ex

or a guy who comes in with a gun." The CIO asks whether it would be worth reallocating your hard-won funding—originally intended to hire three new security personnel—to purchase metal detectors. Furthermore, the CIO suggests that she plans to take the issue to the CEO to ensure swift action is taken.

There are numerous immediate, low-cost—if not free—resources available to security professionals.

If staff are not feeling safe, some steps will need to be taken. However, while the concerns of the CIO and staff are important, your experience tells you the suggestions are unlikely to address the root issue. Instead, they will probably needlessly disrupt the current risk mitigation implementation plan. You believe there are better approaches to take, and you seek to make a case for them.

The key is finding the right course of action—one that maximizes current resources, does not unduly demand new resources, and for which an effective case can be made. This is where readily available research comes into play.

CREDIBLE SOURCES

You do not have to become an academician—or even be particularly tech-savvy—to access research relevant to informing strategic security decisions. In fact, the skills needed to conduct effective research parallel those utilized by effective security professionals.

During the initial stages of an investigation, the security professional narrows the list of individuals to either

interview or consult, making the most of limited time and resources.

Likewise, when engaging in research, it is important to have a reliable and relevant pool of sources, particularly in a world where a simple Internet search can yield hundreds of thousands of hits.

Begin by narrowing down your search with some basic parameters. The research you use should be recent—at minimum published within the last 10 years, ideally within the last five.

Bear in mind that professional journals, which are peer reviewed, inherently provide a greater level of quality control compared to other sources, such as blogs, newspapers, or magazines. If you find information in a more informal source, such as a news article about a research report, it is always best to verify the information from the original source.

For example, a Google search of the murder–suicide referenced by the hypothetical CIO unearths research published by the Johns Hopkins Office of Critical Event Preparedness and Response (Hospital-Based Shootings in the United States: 2000 to 2011). The report confirms that most hospital-based active shooter deaths transpire outside of the physical facility, suggesting that metal detectors would be of limited use in preventing this type of violence. This research can be used to justify an objection to reallocating funding earmarked for personnel to metal detectors.

The Hopkins research also confirms that most hospital-based active shooter incidents target a specific victim, with interpersonal or domestic violence between a staff member and the shooter as one of the most common precipitating dynamics. This validates staff's concerns: Employees are vulnerable to coworkers who may be experi-

encing interpersonal relationship conflict. Addressing staff perceptions of their own vulnerability is equally critical to the security professional's success in creating a safe environment.

Beyond Internet searches, traditional academic research is also within your reach. With an increasing number of colleges and universities offering security programs or majors, security and risk management professionals are in demand as adjunct professors or affiliated faculty. These appointments often are associated with access to a significant number of e-journals in a variety of topics and fields, so it is also beneficial to inquire about this access if accepting one of these positions.

If you are not directly affiliated with a college or university, cultivating relationships with those who might be willing to access this research on your behalf—whether colleagues or interns—is beneficial. If you find a particularly relevant research article, you can also generally purchase or rent the article online from the publisher for a relatively nominal fee.

Consider taking on an intern to assist with research for your program. Internships are important avenues of experience for graduate or undergraduate students and often excellent resources in research assistance.

Additionally, interns do not need to be enrolled in a security program. There are many opportunities for research in behavioral psychology and sociology that would link well with studying human reactions during adverse events. Hiring a research intern outside of the security profession can broaden your view of the issue and create a stronger business case that resonates with nonpractitioners.

Authors of articles in professional journals are required to be transparent about their research endeavors. Consequently, most research articles include an abstract that

briefly summarizes the research and its findings, an overview of the issue and why it is important, details about the research methodology, details about the findings, a discussion section, and a conclusion. Unless you have an interest in becoming a researcher yourself, you can skip the detailed methodology sections and usually find the information you seek in the abstract and discussion sections. The overview often also provides a wealth of supplemental content regarding an issue.

Finding evidence-based practices does not need to be a solitary endeavor. Professional networks, including ASIS International, also provide support. Asking fellow security practitioners for input or trusted research sources is a valuable force-multiplier when developing a reasoned business case for security solutions. Recent discussion posts on an ASIS Open Forum, for example, suggested several evidence-based active shooter training resources geared toward civilian populations (REACT Smarter Civilian Active Shooter Response Instructor Training Program and Civilian Response to Active Shooter Events).

CONTEXT

Although security plans often adopt an all-hazards approach to addressing incidents, research can assist in identifying context-specific nuances that can help inform resource allocation, training plans, and intervention strategies.

The active shooter training programs referenced above are civilian-focused and would not necessarily translate as well when training security staff with law enforcement or military backgrounds. Likewise, such training would not be appropriate in addressing middle school students' safety concerns. Searching for studies specific to middle school security, however, quickly yields advice on practical and effective bystander intervention programs. It also

provides relevant facts to use in community education and awareness campaigns, such as the prevalence rates for mass shootings, which are frequently subject to distortion given their shock value and media attention.

A single research article can lead to useful data.

Research can also assist the security professional seeking to engage in more-targeted violence prevention. For example, a basic search of "middle schools" and "school shootings" in the U.S. National Center for Biotechnology Information's online research archive, PubMed, yields research on the contagion effect of these events and the window during which copycat acts are most likely to occur. This, in turn, can assist in informing the security response. For example, security leaders can suggest allocating limited resources toward the retention of additional personnel during the time period at highest probability for similar acts—two weeks, according to the research.

Another way research can be contextualized is by providing information most relevant to your audience. If discussing active assailant preparedness with the chief financial officer for a public school system following a string of shootings, for example, quantifying the additional personnel costs during the contagion risk period is both concrete and justified by the research.

APPLICABILITY

A single research article can lead to useful data. The process of chasing down supplemental information, however, can result in data paralysis. This phenomenon occurs when the data becomes the focus rather than a means to an end,

obscuring the original problem and hindering engagement in needed action.

Returning to the hypothetical hospital security example, reviewing bystander intervention literature with research relating to four D methods (direct, distract, delegate, and delay) uncovers a relevant violence intervention strategy that translates well to a hospital environment. Conversely, the same search results brought up a successful gun prevention program targeting urban youth and physical self-defense programs for survivors of sexual assault—clearly not pertinent to the goal of supporting hospital staff.

As in other aspects of security decision making, the ability to quickly set aside irrelevant information is as important as competently utilizing applicable data.

AVOIDING TUNNEL VISION

An additional benefit of incorporating research in decision making is that it helps avoid confirmation bias—the all-too-human tendency to "see what we believe" or, more accurately, to only heed information that aligns with what we already think.

Our minds use "templates" to prevent us from becoming overloaded by the incredible amount of information and stimuli we are subject to on a daily basis. If we experience something new that is similar to something we learned in the past, we quickly file the new experience in the existing template and move on with our day. Our typical "top-down" cognitive processing can be useful, such as when we use context clues or patterns to decipher difficult handwriting or fill in missing letters.

This highly efficient way of processing the world also has a potential downside—when we file new experiences with previous ones, we assume that the new experiences will share the characteristics and behaviors of the prior ones.

Research has repeatedly shown that individuals engaged in familiar tasks, particularly when multitasking, fail to perceive hazards in their midst, including oncoming traffic or potential assailants. And in the case of people, we tend to make similar associations: If a stranger reminds us of our kindly grandmother, we will tend to be favorably disposed to like them. If the stranger reminds us of a litigious neighbor, we are more likely to take offense. What we have previously learned or thought—even if it is inaccurate, incomplete, or irrelevant—influences future thinking.

The impact of this process on security is often seen after mass shooting events, when the public demands a response that addresses a perceived association between extreme acts of violence and mental illness. However, research shows that a minority of lone actors (32 percent) and significantly fewer group actors (3 percent) suffer from a mental illness. Left unchallenged, the bias that links mental illness with mass violence could result in threat assessments that overlook nuanced—and more relevant—risk factors, such as situational stressors, social isolation, and an absence of constraints.

LIMITATIONS

Do not generalize research beyond its limits. Risk factors for violence in hospital settings, for example, vary by country. A quick Google search of workplace violence rates against hospital staff in Europe yields a National Institutes of Health article about assault prevalence rates across several nations. Knowing that the annual prevalence rate for assault among hospital workers in Germany is 56 percent, compared to 11.5 percent in Italy, suggests that the probability for assault on German hospital workers warrants prioritization of violence prevention efforts to support these staff. In Italy, however, other risks could

outweigh workplace violence. Of course, location is only one context that merits consideration when determining the relevance of research data or findings.

Also consider whether the research concerns relevant or similar facilities. For example, regarding settings that are open to the public such as an entertainment venues, transportation hubs, retail stores, or other public spaces, there is growing research on the ways in which social media has created disembodied bystanders—people who will record violent incidents rather than intervene or call for help—and effective strategies for encouraging a more active, security-conscious response. This may not be applicable in an area with restricted access, such as an access-controlled office building or factory.

In general, the more closely the population studied matches the population you are seeking to protect, the more useful the research will be.

EXPANDING OPTIONS

Perhaps the most significant benefit to combining research with professional experience and judgment is that it expands options for effectiveness. Research confirms what works, or it presents better solutions.

The security professional seeking to engage hospital staff in strengthening workplace violence prevention efforts, for example, can demonstrate successful efforts with existing research and internal metrics. A simple and effective research approach is the pre- and post-test design (see the sidebar, "Practice into Research," for more information).

In the hypothetical hospital, the security leader can survey staff on what factors they believe pose the greatest risk of workplace violence—such as patients, domestic violence, or outside violence—as well as their knowledge of effective interventions. This provides a baseline for

gauging staff members' understanding of the two elements of violence risk assessment: forecasting probable acts of violence at the hospital and identifying appropriate practical interventions for that setting.

Then, provide factual data regarding violence risk (such as prevalence rates for violence subtypes and historic reports of violence in various departments) and evidence-based training in violence prevention and risk mitigation (such as early identification and notification of peer substance use, domestic violence reporting, and resiliency building). The original survey is re-administered after training to identify the improvements made in the staff's levels of knowledge, preparedness, and anxiety about their safety.

By applying research—particularly in areas that are extensively and continuously studied, such as risk assessment—security's efforts remain informed, contemporary, and dynamic.

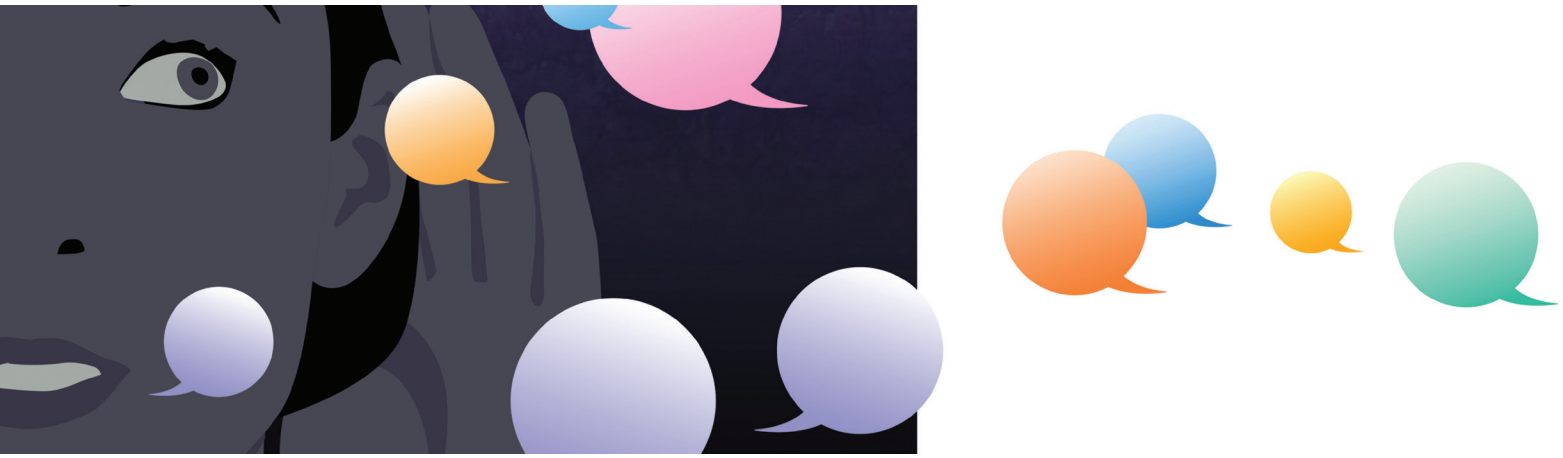
DR. DIANA M. CONCANNON IS A FORENSIC PSYCHOLOGIST, ASSOCIATE PROVOST AT ALLIANT INTERNATIONAL UNIVERSITY, AND DEAN OF THE CALIFORNIA SCHOOL OF FORENSIC STUDIES. SHE IS A MEMBER OF ASIS INTERNATIONAL'S PROFESSIONAL DEVELOPMENT AND SCHOOL SAFETY AND SECURITY COUNCILS. MICHAEL CENTER IS A REGIONAL SECURITY ADVISOR FOR THE UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY BASED IN BRUSSELS, BELGIUM. HE IS VICE CHAIR OF THE ASIS PROFESSIONAL DEVELOPMENT COUNCIL AND VICE CHAIR FOR SUBJECT MATTER EXPERTISE OF THE GLOBAL TERRORISM, POLITICAL INSTABILITY, AND INTERNATIONAL CRIME COUNCIL. THE VIEWS EXPRESSED IN THIS ARTICLE ARE THE AUTHORS' OWN AND ARE NOT REFLECTIVE OF THEIR ORGANIZATIONS.

SECURITY MANAGEMENT

The Hard Truth About Soft Skills

We asked five security industry recruiters about the importance of soft skills. The short answer: communication abilities and emotional intelligence are crucial for managers.

By Mark Tarallo



"Hard skills will get you the interview—soft skills will get you the job." David Lammert, a 17-year veteran of security industry recruiting and current president of Pinnacle Placements, is a big believer in this adage. And he's not the only one.

"We have all seen situations where the decision to hire—when two or more candidates present the same level of hard skills' strength—is made with soft skills as the differentiator," says recruiter Rebecca Bayne, the president of Bayne Consulting & Search Inc. who specializes in staffing the security integration space. "It triggers the gut-level instinct of the hiring manager and determines who will get the offer."

"And soft skills," Lammert adds, "will also determine how well you perform in the job, and how long you do it."

Other recruiters are on the same wavelength as Lammert and Bayne when it comes to the importance of soft skills. Although hard skills like specialized security knowledge

and technical expertise in an industry subsector are still essential, a successful leader needs a broad soft skill set to navigate different managing situations, recruiters say.

Given the importance of soft skills, Security Management asked five industry recruiters to discuss which skills they believed to be most crucial for security managers both current and aspiring. In these discussions, two broad soft skill sets—communication ability and emotional intelligence—came up time and again. Recruiters explained how

"The most important soft skill is communication. It's the foundation of every other soft skill," says Jane Snipes, managing partner at NorthStar Recruiting.

these skills apply to specific managerial situations. They also shared some general employment trends and discussed the soft skills of the future.

COMMUNICATION

For many recruiters, communication ability reigns supreme when it comes to soft skills.

"The most important soft skill is communication. It's the foundation of every other soft skill," says Jane Snipes, managing partner at NorthStar Recruiting.

"In my experience, communication skills are paramount to one's capability to execute and deliver the day-to-day requirements of leadership and having oversight for a team, small or large," Bayne says.

In Lammert's view, communication skills are an umbrella that covers several individual talents that have many applications, both inside and outside the firm.

"It's such an important skill set—there's so much interaction internally [in a company]," he says. "It covers speaking, active listening skills, presentation skills, and more."

For example, a security manager's speaking and conversation skills will be a huge asset in working with vendors and external business partners outside the company, as well as technical staffers, C-suite executives, and the CEO within the firm.

"In this fast-paced business environment, the ability to communicate clear and concise messages is crucially important," Lammert explains.

Another key asset under the communications umbrella is the ability to be an effective storyteller. For an aspiring security manager, the value of this skill begins in the interview—the ability to communicate and frame one's career progression as a purpose-driven narrative that is gaining momentum is "critically important for a successful candidate," Lammert says.

After the manager lands the job, storytelling continues to be an asset. "It also helps you become an influencer wherever you are in the organization," he adds.

Another key asset under the communications umbrella is the ability to be an effective storyteller.

Communication skills are also crucial for a manager in working with direct reports, recruiters say. Successful managers have a desire to coach, facilitate, and develop talent, and this takes continual—and sometimes nuanced and sensitive—communication.

"In general, those who achieve the greatest success in their careers have a genuine interest in those around them and are skilled in communicating," Snipes says.

For years, employee surveys such as the ones taken by the Gallup company have found versions of "I don't like working for my boss" as the most common reason for people leaving a job.

Although there may be various reasons why a manager is disliked, a common one stems from the manager's failure to adequately communicate how valuable an employee's contributions are. The employee winds up feeling undervalued and unappreciated, Snipes says.

"People don't leave companies, they leave managers, and the common factor lacking in those managers who chase away great talent is the ability to genuinely appreciate the value an individual has to the company and to consistently communicate that value," she explains.

For managers, the lesson here is not only that communication skills are vital, but that they need to be consistently used. Sometimes, otherwise articulate managers will fail to communicate due to being too self-absorbed—they are occupied with their own career advancement and impressing the organization's senior leaders, rather than attentive to their direct reports. "Many managers focus on themselves instead of serving those they lead," Snipes says.

Finally, there's another communication-related skill that's a key asset for security managers—the ability to establish a safe space for honest two-way communication, says Kevin Spagone, vice president of Reitman Security Search/Reitman Personnel, Inc.

This type of communication needs to be embedded in the company's culture, so that employees feel comfortable in offering honest views without fear of reprisal or relationship damage, he explains. Not only will this help employee retention, it will also help the firm's reputation among potential employees, which will help recruitment efforts.

"Leaders who foster a culture where open, honest two-way feedback is the norm," he explains, "are savvy enough to realize that this gives them a competitive advantage in the marketplace."

EMOTIONAL INTELLIGENCE

Recruiter Stephanie Campbell of Security and Investigative (SI) Placement, LLC, finds that, besides communication skills, emotional intelligence has become an important attribute for candidates in the current security management job market. "I am finding more and more interest in that skill set," she says.

Emotional intelligence (often abbreviated as EQ) is the ability to perceive another's emotions, reactions, and perspective, and to handle interpersonal relationships judiciously and empathetically. In the world of the security manager, it has many applications, recruiters say.

Campbell illustrates by relating a question she asks clients when trying to go beyond the job description to get a strong handle on what type of candidate would be a good fit.

"When we're working with a client, we will sometimes ask, 'What is it that's not in the description that you are looking for?'" she says. "What's that extra bit, that's sort of between the lines?"

The answer is often "a lot of EQ skills." These include working well as a teammate, empathetic listening, building consensus, and an ability to be persuasive and to motivate.

Security professionals are rarely required to answer the question, "Why are we doing this?" she says. Emotional intelligence is a huge asset for a manager who is trying to explain this in such a way that will motivate teams to embrace initiatives, she continues.

EQ is also an asset in the interview itself, because it helps candidates demonstrate their value, Snipes adds.

"The high EQ ones are fine-tuned to how they are perceived," she says. "They're not just leaning on their laurels. They have actively done the research on the company, and so they can give examples of potential contributions that are directly relevant.... They are making really good impressions."

Lammert is also convinced of the value of emotional

intelligence, and says it bolsters a manager's communication skill set.

For example, managers with high EQ are aware of their audience; they know that different employees have different learning styles and interests, and they can tailor messages and delivery to fit each employee.

"One case may call for more of a visual message, another case more of a technical type of message," he says.

SKILL GAPS

While there is a near-uniform consensus on the importance of communication ability and emotional intelligence for security managers, these skills are hard to find in some candidates, recruiters say. Some observe that overreliance on technology is eroding person-to-person communication.

"Communication skills are becoming seriously lacking," Snipes says. "We've become a society, a world, so focused on communicating electronically that the ability to strike up a conversation in person with another human being is becoming a lost art, particularly with the younger generations."

We've become a society, a world, so focused on communicating electronically that the ability to strike up a conversation in person with another human being is becoming a lost art, particularly with the younger generations.

"The more the younger generations communicate electronically," she adds, "the less practice they'll have communicating in person and the more often that lack of skill will be noticed."

Bayne voices a similar view. "I believe that some of the technology we use on a daily basis has changed our approach to

communication and made some of us a bit lazy," she says. "This has most clearly affected younger generations who have learned to communicate more frequently with those tools, instead of using traditional verbal or written communication."

And Snipes sees another communication-related issue that is becoming more common with younger professionals. As the use of LinkedIn becomes ubiquitous in the business and employment world, some younger candidates are using it as a social network instead of a professional network.

"These users are using profile pictures from social situations, with nary a thought as to how the picture might be perceived by a prospective employer," Snipes says.

Her advice is simple: keep professional photos professional. "I suggest avoiding the four Bs in profile pictures—no beer, boats, baseball caps, or other people's body parts (that is, no one else's chin, arm, hair, or shoulder)."

Communication gaps are not the only deficiency, recruiters say. In the area of emotional intelligence, self-awareness can be a subtle yet important attribute for a security manager to have, but some lack it, Lammert says.

"It's that seeking of feedback, the willingness to admit mistakes and take responsibility for actions," he says.

One possible reason for that lack is that, unlike other skills that can be linked to performance metrics, "self-awareness is not as easy to measure," and not as frequently talked about, he adds. Still, it is a great quality to have, and self-aware managers often realize the importance of continuous growth.

"It can also drive a desire for development, and a desire to take on leadership roles," he explains.

Another subtle-yet-valuable soft skill that seems to be lacking in many security managers these days is the ability to question assumptions, says Spagone. With technology and analytics developing at lightning speed, a successful manager can't hold on to traditional ways of solving problems.

"There is a key subtle difference in the ability to identify a challenge without assuming that it can be solved the same way it was a year or two ago," Spagone explains.

Take for example a security manager who has found that one component of the firm's security program has fallen out of compliance. That manager should not assume that the traditional methods of addressing that problem are still valid.

"They must consistently question how decisions are reached, while still adhering to consistent standards, such as regulatory requirements," he says.

SKILL SETS

But while some security managers may need to fill skill gaps, others pulled together several soft skills to build a skill set that is especially effective in today's industry.

For example, Bayne cites the common industry reality that companies continue to try to do more with less, even though the pace of business continues to speed up.

"Anyone in our industry who is good at what they do has more on their plate than ever, and is busier than they have ever been before," she says. "Because of that, the job needs to be done right the first time, for efficiency in productivity and to maintain the highest level of customer retention."

Security managers who can survive, and even thrive, in this environment usually combine communication skills with the ability to work under pressure, a knack for troubleshooting, and an insistence on maintaining integrity and a code of ethics so no corners are cut, Bayne says.

Spagone mentions another persistent reality in the industry—the view held by some company leaders that security is a cost center that is a distraction (albeit a necessary one) from the overall business goals and financial targets of the firm.

In this environment, certain security managers have the right combination of business understanding, executive pres-

ence, and a focus on vision, goals, and transparency, and this skill set helps top executives think of security in a less limited way.

"It's about breaking the mold," Spagone says.

Bayne agrees, and adds that some of the soft skills in a desired skill set evolve over time. She offers the example of executive presence.

"The executive presence which now seems to garner the highest level of respect is very different than it was in previous decades," she explains. "More than ever, leaders are expected to be transparent, approachable, and in the trenches with their teams, rather than delivering orders from above."

Furthermore, Bayne cites another important relevant trend in the industry: an organizational focus on developing a strong and distinctive culture. In that environment, managers who have combined the soft skills of coaching, team building, and teaching are often sought after.

"Coaching, team building, and teaching often tie back to specific areas of corporate culture, and because they are being demanded from the most recent additions to the talent pool, they are in the spotlight more than ever," she explains. "They are now considered critical by both candidates and companies."

Finally, Spagone says it is important to keep in mind that the combination of soft skills needed will also depend on the circumstances surrounding the position being filled.

"Companies and cultures are unique. And all new hires are about addressing an organizational challenge of some kind," he says.

SKILLS OF THE FUTURE

Looking forward, the soft skill set of coaching, team building, and teaching will continue to be vital for the security managers of the future, but with a new twist, Spagone

says. He illustrates this by explaining a recent trend in the recruiting industry.

"We used to struggle with candidates that were heavily institutionalized–leaders who had been successful inside of their own insular corporate cultures, but who were unable to adapt in a different environment," he explains. "They were not agile enough to be effective in a new or different organization."

But this is becoming less common, as businesses are more interconnected than ever. To compete, companies must be increasingly agile.

Team building will still be crucial, but in a more strategic and fluid way, so that interdependent teams are staffed with members possessing portable skills. They may trade members, interlock if necessary, and work at an increasingly rapid pace, and managers must be able to make strategic decisions on the fly and nimbly rearrange all the pieces.

"Leaders must continue to understand where they need to add to their roster," Spagone says, "and what skills can be groomed, what can be replaced or outsourced, or shared among their team—and themselves."

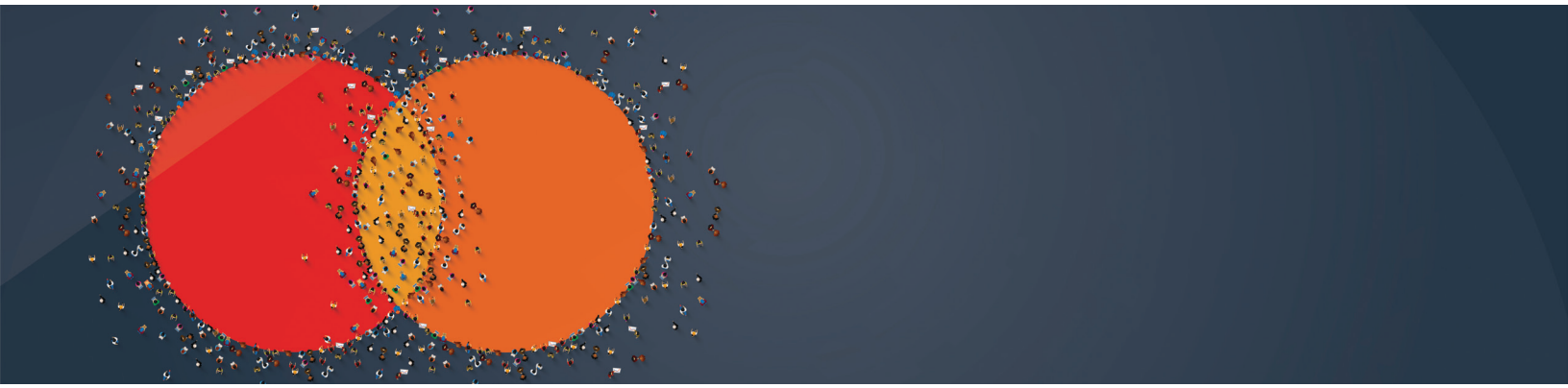
MARK TARALLO IS SENIOR CONTENT MANAGER AT SECURITY MANAGEMENT. CONTACT HIM AT MARK.TARALLO@ASISONLINE.ORG. CONNECT WITH HIM ON LINKEDIN.

SECURITY MANAGEMENT

A Converged Campagin

With a converged security team, Mastercard is taking a unified approach to addressing risks and educating its workforce to reduce threats.

By Megan Gates



We are all in this together. That was theme that swept the world in the wake of the coronavirus pandemic.

The sentiment was reiterated at Mastercard after CEO Ajay Banga released a letter to the financial institution's community, reiterating its commitment to serving its customers, employees, and society as a whole during this unprecedented time.

"At Mastercard, our focus has always been on helping to build a more connected world, and in today's environment, this is more important than ever," Banga wrote. "We remain committed to that cause and are moving forward in a way that supports human safety and global efforts for sustainability now and recovery in the future. We are in this with each and every one of you for the long haul and I am confident that, as long as we keep plugging in to our basic human decency, we will emerge from this and find new strengths and growth we never imagined."

A core component of this crisis response is ensuring that

Mastercard employees are safe and can continue their work securely, Banga added.

"During this time of uncertainty, we pledged to all our employees that there will be no layoffs related to the COVID-19 crisis in 2020," he wrote. "And we've initiated several temporary policies according to guidance from regional authorities, international health organizations, and our employees' own concerns and comfort levels, including working from home, split working schedules, restricted or postponed travel, among others."

This approach models a philosophy held at Mastercard that safety and security are not just the responsibility of the security department, but of all employees who play a valuable role in protecting the organization's assets, says Ron Green, chief security officer for Mastercard.

"In the past, the organization would have felt that the security team takes care of that—we have other stuff to do," Green explains. "Today, security is something that we all have to do at Mastercard."

SECURITY PHILOSOPHY

Corporate security leaders have discussed the idea of converging their physical security and cybersecurity teams for more than a decade. Roughly 25 percent of organizations in certain parts of the world have taken that step—sometimes also including business continuity—according to research by the ASIS International Foundation, The State of Security Convergence in the United States, Europe, and India.

The benefits of this approach include greater ability to align security strategy with corporate goals, greater communication and cooperation, more efficient security operations, and more visibility and influence with the board and C-suite, according to the report.

Mastercard has merged its physical and cybersecurity teams to better address threats that the financial institution faces.

"Our adversaries, they don't think that way—cyber and physical being separate—they just attack," Green tells Security Management. "They don't have that artificial boundary to hold them or slow them up. They don't care. Because we're combined, we just think about security."

Other organizations are coming to a similar conclusion—especially when it comes to preventing fraud. For example, the U.S. Secret Service recently merged its Electronic Crimes Task Forces and Financial Crimes Task Forces into a single network known as the Cyber Fraud Task Force.

"Online payments and banking are now globally pervasive, credit card numbers and personal information are illegally sold on the Internet and Dark Web, and cryptocurrencies have become one of the primary means by which criminals launder their illicit profits," the Secret Service said in a press release. "No longer can investigators effectively pursue a financial or cybercrime investigation without understanding both the financial and Internet sectors, as well as the technologies and institutions that power each industry."

Mastercard benefits from having a CEO who buys into the philosophy of convergence, Green says. Along with being the CEO, Banga is the co-founder of the Cyber Readiness Institute, served on U.S. President Barack Obama's Commission on Enhancing National Cybersecurity, and led discussions at the Business Roundtable on security matters. Banga's interest in security—and in making it a core component of Mastercard's mission—has helped Green and his team receive buy-in from other executives for their work.

Green briefs the executive leadership team on security threats and provides data about risks to their specific teams.

"The ability to report on the status of their teams' susceptibility, that gives the executives data to go in and talk to

their teams," Green says. "If you want to get your executives engaged, you have to make them knowledgeable and provide them with how they can help."

These actions have also encouraged the mind-set that security is everyone's responsibility at Mastercard—not just the security team's domain. This has become especially critical in recent years as social engineering and phishing

"Companies are then compromised, and data is stolen or altered. But it starts with people not being focused on security."

have become some of the main attack methods for malicious actors to infiltrate organizations and compromise networks. (See "A Patrol Problem," Security Management, August 2020)

"One of the principal reasons we're focused on security as everybody's responsibility is if you look at the way the threat moves, many breaches today start from compromising an unintentional insider through phishing and social engineering them to do the wrong thing," Green says. "Companies are then compromised, and data is stolen or altered. But it starts with people not being focused on security."

RAISING AWARENESS

Not everyone is a security expert. But all employees have some degree of access to corporate networks and sensitive data that if compromised could place the organization at risk. All employees need to have some basic security knowledge and receive training to help reduce risk, Green says.

To help educate the general workforce, Mastercard created its Secure It awareness program that focuses on one topic each month. The overarching themes and programs are

developed in house, but Mastercard works with a video company to produce sketches that are then shared through its Secure It TV programming.

"It's got a usual host of characters that people have become accustomed to handling a security issue, such as connecting to Wi-Fi in a coffee shop or managing passwords," Green says.

Secure It also brings in outside speakers, such as Frank Abagnale, who operated as a con man from the time he was 15 until caught by authorities at age 21 and whose story was dramatized in the movie Catch Me If You Can. He later worked for the U.S. federal government and is now a security consultant for the FBI academy and private organizations.

These speakers share information on high-profile security topics, as well as security risks that impact employees' everyday life—such as how to secure your home Wi-Fi network like a professional.

"We do a lot to bring it home," Green says. "If someone tries to trick you into giving up information, or breaking into networks, that puts you and your personal information at risk. We gear up people to think about security in their everyday home life."

"The technical guys are never going to articulate it in a way to change the mind-set—this is where we need HR, communications, operations, and others to help out," he adds.

The security team also partnered with human resources and communications to help articulate and explain technical concepts to a nontechnical audience, says Neil Parker, Mastercard's business security officer, employee digital experience, and member of the ASIS International Young Professionals Council.

"The technical guys are never going to articulate it in a way to change the mind-set—this is where we need HR, communications, operations, and others to help out," he adds.

Additionally, Mastercard conducts regular phishing training and test campaigns. Mastercard previously only ran these campaigns twice a year, but recently began conducting them every month for all employees—including the CEO and his direct reports.

"We've established standards around acceptable behavior, and there is training if you fail the tests," Green says. "There are also consequences associated with it because our employees are accountable for their conduct. We have a 'three strikes and you're out' policy."

In his monthly briefing with the CEO and senior executives, Green will share the results from previous phishing exercises so they can take that data back to their teams.

"Those executive leaders talk to their teams about the importance of paying attention, having the right hygiene when it comes to protecting Mastercard," Green says.

This became especially critical as many Mastercard employees made the transition to working fully remote during the coronavirus pandemic. In March and April, Mastercard briefly paused its phishing tests to employees. It also beefed up briefings and information for employees to help them secure their new home office space and help reduce risk to Mastercard.

"With the pivot to put everybody at home, the threat landscape changed," Green says.

Through a Secure It challenge, Mastercard provided videos on securing home routers, things to consider when using an Alexa or Google Home system, and more. Employees who participated in the challenge received a pin for their efforts, and Green says that the voluntary program has caught on.

"I think the transition has been easy for us," says Parker. "We never wanted to look at just security within our walls but security being a way of life. We enable our employees to connect to work from everywhere. You need to be thinking about security everywhere, as your normal way of life."

Programs like Secure It have helped employees see the security team as a business enabler instead of a police force for the organization, Parker adds.

"When we look at legacy and how to get employee buy-in, the big change for corporate security is not being seen as policing the organization," he explains. "We've helped

Mastercard has also made tools available to help smaller organizations think through core security components, such as asset management, anti-malware, and network scanning

lead the way with that by combining the cyber and physical teams, and by doing that, it's changed us from being the police to being a partner and business enabler—expediting buy-in."

And these programs have helped to make a difference in protecting Mastercard. Banga issued an ambitious goal to the security team: reduce phishing attempt click-through rates to a 1 percent average across the organization. After testing nearly every month, Parker says Mastercard is very close to meeting that goal—despite increasing the difficulty of its testing.

Mastercard is also sharing its best practices with smaller and medium-sized businesses that cannot afford a security apparatus as robust as its own.

"We partnered with the Global Cyber Alliance and created the Cyber Readiness Institute to help provide best practices for small and medium businesses," Green says.

Mastercard has also made tools available to help smaller organizations think through core security components, such as asset management, anti-malware, and network scanning.

"We give you the why of why you need to do it, and also provide videos and free tools so you can manage your assets," Green explains. "We're giving you the ability to raise the game and protect yourself."

MEGAN GATES IS SENIOR EDITOR AT SECURITY MANAGEMENT. CONNECT WITH HER VIA LINKEDIN OR AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.

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.